

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-288376

(43)Date of publication of application : 04.10.2002

(51)Int.Cl.

G06F 17/60

(21)Application number : 2001-087300

(71)Applicant : SANYO ELECTRIC CO LTD

(22)Date of filing : 26.03.2001

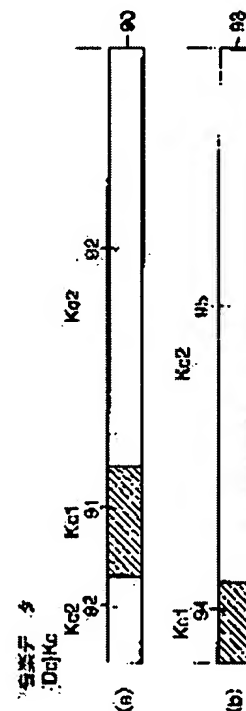
(72)Inventor : HORI YOSHIHIRO
HIOKI TOSHIAKI

(54) CONTENTS PROVIDING METHOD AND DATA REPRODUCING DEVICE AND DATA RECORDING DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a contents providing method for distributing enciphered contents data divided into a plurality of blocks and a plurality of licenses for decoding and reproducing the enciphered data included in those blocks.

SOLUTION: Enciphered contents data 90 or 93 obtained by enciphering music data are composed of trial enciphered music data 91 or 94 and main enciphered music data 92 or 95. The enciphered music data 91 and 94 are decoded by a license key Kc1, and the enciphered music data 92 and 95 are decoded by a license key Kc2. A distributing server holds the enciphered contents data 90 and 93 and the license keys Kc1 and Kc2, and distributes the trial enciphered music data 91 or 94 and the license key Kc1, and the main enciphered music data 92 or 95 and the license key Kc2 in this order in response to a distribution request.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of

THIS PAGE BLANK (USPTO)

rejection]

[Kind of final disposal of application other than
the examiner's decision of rejection or
application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's
decision of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-288376

(P 2 0 0 2 - 2 8 8 3 7 6 A)

(43) 公開日 平成14年10月4日 (2002. 10. 4)

(51) Int. Cl.	識別記号	F I	テ-コ-ド (参考)
G06F 17/60	142	G06F 17/60	142
	ZEC		ZEC
	302		302 E
	512		512

審査請求 未請求 請求項の数13 O L (全25頁)

(21) 出願番号 特願2001-87300 (P 2001-87300)

(22) 出願日 平成13年3月26日 (2001. 3. 26)

(71) 出願人 000001889

三洋電機株式会社

大阪府守口市京阪本通2丁目5番5号

(72) 発明者 堀 吉宏

大阪府守口市京阪本通2丁目5番5号 三

洋電機株式会社内

(72) 発明者 日置 敏昭

大阪府守口市京阪本通2丁目5番5号 三

洋電機株式会社内

(74) 代理人 100064746

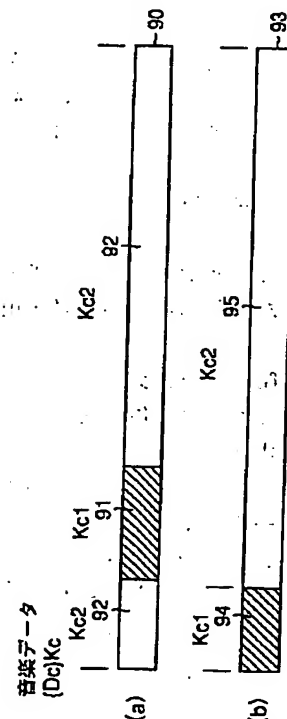
弁理士 深見 久郎 (外3名)

(54) 【発明の名称】 コンテンツ提供方法、データ再生装置、およびデータ記録装置

(57) 【要約】

【課題】 複数のブロックに分離された暗号化コンテンツデータと、複数のブロックに含まれる暗号化データを復号および再生するための複数のライセンスとを配信するコンテンツ提供方法を提供する。

【解決手段】 音楽データを暗号化した暗号化コンテンツデータ 9.0 または 9.3 は、試聴用の暗号化音楽データ 9.1 または 9.4 と本体用の暗号化音楽データ 9.2 または 9.5 から成る。暗号化音楽データ 9.1、9.4 はライセンス鍵 Kc1 によって復号され、暗号化音楽データ 9.2、9.5 はライセンス鍵 Kc2 によって復号される。配信サーバは、暗号化コンテンツデータ 9.0、9.3 およびライセンス鍵 Kc1、Kc2 を保持しており、配信要求に応じて試聴用の暗号化音楽データ 9.1 または 9.4 およびライセンス鍵 Kc1、本体用の暗号化音楽データ 9.2 または 9.5 およびライセンス鍵 Kc2 の順序で配信する。



【特許請求の範囲】

【請求項 1】 コンテンツデータを暗号化した暗号化コンテンツデータの取得要求を受信する第 1 のステップと、

前記第 1 のステップにおいて受信した取得要求に応じて、前記暗号化コンテンツデータを提供する第 2 のステップと、

前記暗号化コンテンツデータの一部に対応し、かつ、前記一部を復号するための第 1 のライセンスの提供要求を受信する第 3 のステップと、

前記第 3 のステップにおいて受信した提供要求に応じて、前記第 1 のライセンスを提供する第 4 のステップと、

前記第 1 のライセンスと異なり、かつ、前記暗号化コンテンツデータの前記第 1 のライセンスに対応しない他の一部に対応し、前記他の一部を復号するための第 2 のライセンスの提供要求を受信する第 5 のステップと、
前記第 5 のステップにおいて受信した提供要求に応じて、前記第 2 のライセンスを提供する第 6 のステップと、

前記第 2 のライセンスの提供に対して課金処理を行なう第 7 のステップとを含むコンテンツ提供方法。

【請求項 2】 前記暗号化コンテンツデータ、前記第 1 のライセンス、および前記第 2 のライセンスが同じサーバから配信される、請求項 1 に記載のコンテンツ提供方法。

【請求項 3】 前記暗号化コンテンツデータ、および前記第 1 のライセンスが第 1 のサーバから配信され、前記第 2 のライセンスが前記第 1 のサーバと異なる第 2 のサーバから配信される、請求項 1 に記載のコンテンツ提供方法。

【請求項 4】 前記暗号化コンテンツデータ、および前記第 1 のライセンスは、記録媒体を介して前記第 1 のサーバに供給される、請求項 3 に記載のコンテンツ提供方法。

【請求項 5】 前記暗号化コンテンツデータが第 1 のサーバから提供され、前記第 1 および第 2 のライセンスが前記第 1 のサーバと異なる第 2 のサーバから配信される、請求項 1 に記載のコンテンツ提供方法。

【請求項 6】 前記暗号化コンテンツデータは、記録媒体を介して前記第 1 のサーバに供給される、請求項 5 に記載のコンテンツ提供方法。

【請求項 7】 前記第 3 のステップにおいて、前記提供要求とともに認証データを受信し、前記認証データが認証されると前記第 1 のライセンスを提供し、
前記第 5 のステップにおいて、前記提供要求とともに認証データを受信し、前記認証データが認証されると前記第 2 のライセンスを提供する、請求項 1 から請求項 6 のいずれか 1 項に記載のコンテンツ提供方法。

【請求項 8】 複数のブロックから成る暗号化コンテンツデータを前記複数のブロックに対応する複数のライセンスによって復号して再生するデータ再生装置であって、

前記暗号化コンテンツデータ、および前記複数のライセンスが記録されたデータ記録装置とのやり取りを行なうインタフェースと、

指示を入力するための操作部と、

前記暗号化コンテンツデータを前記複数のライセンスによって復号して再生するコンテンツ再生部と、

制御部とを備え、

前記制御部は、前記コンテンツ再生部において、前記暗号化コンテンツデータを構成する n 番目 (n は自然数) のブロックに含まれる暗号化データが前記 n 番目のブロックに対応する n 番目のライセンスによって復号および再生されているときに、 $n + 1$ 番目のライセンスを前記インタフェースを介して前記データ記録装置から取得して前記コンテンツ再生部に与える、データ再生装置。

【請求項 9】 前記コンテンツ再生部は、

前記 n 番目のライセンスに含まれる n 番目のライセンス鍵を保持する第 1 のライセンス鍵保持部と、
前記 $n + 1$ 番目のライセンスに含まれる $n + 1$ 番目のライセンス鍵を保持する第 2 のライセンス鍵保持部と、
前記第 1 および第 2 のライセンス鍵保持部から前記 n 番目のライセンス鍵と前記 $n + 1$ 番目のライセンス鍵とを選択的に取得し、その取得したライセンス鍵によって対応する暗号化データを復号する復号部と、
前記復号部によって復号されたコンテンツデータを再生する再生部とを含む、請求項 8 に記載のデータ再生装置。

【請求項 10】 前記制御部は、鍵変更情報を前記インタフェースを介して前記データ記録装置から取得し、前記鍵変更情報に基づいて前記 n 番目のライセンス鍵と前記 $n + 1$ 番目のライセンス鍵とを選択して前記復号部に与える、請求項 9 に記載のデータ再生装置。

【請求項 11】 前記データ記録装置から前記複数のライセンスの各々を取得するセッションにおいて、異なるセッションキーを発生するセッションキー発生部と、
前記セッションキー発生部によって発生されたセッションキーを受け、そのセッションキーによって暗号化ライセンス鍵を復号し、その復号したライセンス鍵を前記第 1 または第 2 のライセンス鍵保持部に与えるライセンス鍵復号部とをさらに備え、

前記制御部は、前記セッションキー発生部によって発生されたセッションキーを前記インタフェースを介して前記データ記録装置に入力し、前記セッションキーによって暗号化された暗号化ライセンス鍵を前記インタフェースを介して前記データ記録装置から取得して前記ライセンス鍵復号部に与える、請求項 10 に記載のデータ再生装置。

【請求項 1 2】 前記ライセンス鍵を提供するライセンス配信サーバから前記ライセンス鍵をダウンロードするための通信を行なうデータ送受信部をさらに備え、前記制御部は、前記暗号化コンテンツデータの全部を再生するために必要なライセンスが前記データ記録装置に記録されていないとき、前記データ記録装置に格納されている前記暗号化コンテンツデータに対応する前記複数のライセンスによって再生可能なブロックのみを前記暗号化コンテンツデータの再生順に従って、前記データ記録装置から取得して前記コンテンツ再生部に与え、前記操作部から入力される新たなライセンス鍵の取得指示に従って前記ライセンス配信サーバから前記暗号化コンテンツデータを構成するブロックに対応するライセンス鍵を前記データ送受信部を介して受信し、その受信したライセンス鍵を前記データ記録装置に記録する、請求項 8 に記載のデータ再生装置。

【請求項 1 3】 複数のブロックから成る暗号化コンテンツデータおよび前記複数のブロックに含まれる複数の暗号化データを復号するための複数のライセンスとを記録するデータ記録装置であって、前記複数のライセンスを格納するライセンス領域と、前記暗号化コンテンツデータと、前記複数のライセンスの各々と前記暗号化コンテンツデータを構成する前記複数のブロックとの対応を示すライセンス対応情報とを格納するデータ領域とを備えるデータ記録装置。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】 この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システムにおけるコンテンツ提供方法、データ再生装置、およびデータ記録装置に関するものである。

【0 0 0 2】

【従来の技術】 近年、インターネット等のデジタル情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【0 0 0 3】 このようなデジタル情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【0 0 0 4】 したがって、このようなデジタル情報通信網上において音楽データや画像データ等の著作権者の権利が存在するコンテンツデータが伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【0 0 0 5】 一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介してコンテンツデ

タの配信を行なうことができないとすると、基本的には、コンテンツデータの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【0 0 0 6】 ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録した CD（コンパクトディスク）については、CD から光磁気ディスク（MD 等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体や MD 等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。

【0 0 0 7】 しかも、CD から MD へデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能な MD からさらに他の MD に音楽情報をデジタルデータとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

【0 0 0 8】 このような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【0 0 0 9】 この場合、デジタル情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【0 0 1 0】 そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書とを暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を送信する。そして、暗号化コンテンツデータやライセンス鍵を配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

【0 0 1 1】 最終的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化したライセンスと、暗号化コンテン

ッデータとをメモリカードに送信する。そして、メモリカードは、受信したライセンスと暗号化コンテンツデータとを記録する。

【0012】そして、メモリカードに記録された暗号化コンテンツデータを再生するときは、メモリカードを携帯電話機に装着する。携帯電話機は、通常の電話機能の他にメモリカードからの暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。

【0013】このように、携帯電話機のユーザは、携帯電話機を用いて暗号化コンテンツデータを配信サーバから受信し、その暗号化コンテンツデータを再生することができる。

【0014】暗号化コンテンツデータの配信においては、たとえば、音楽データを試聴用の暗号化音楽データと配信用の暗号化音楽データとに分離し、まず、試聴用の音楽データを配信し、ユーザが試聴用の音楽データを復号および再生して試聴した結果、配信用の暗号化音楽データとライセンスの配信を希望するときに配信用の暗号化音楽データとライセンスを配信することが行なわれている。このような場合、試聴用音楽データは本体用音楽データに比べて音質が劣っていて、仮に、試聴用音楽データをダウンロードしても著作権者の権利を損なわないようになっている。

【0015】

【発明が解決しようとする課題】しかし、ユーザにとつては、試聴用音楽データによって購入しようとする音楽データの特定は可能であるが、提供される配信用音楽データの音質について確認できない。また、試聴用音楽データと配信用音楽データが同一である保証がない。

【0016】このような、問題は音楽データに限らず、朗読データ、教材データ、ビデオデータ、ゲーム等のコンテンツデータの配信において同様に生じる。

【0017】さらには、朗読データ、教材データ、ゲームなどのコンテンツデータにおいては、すべてのデータを一括で購入するのではなく、例えば、朗読データでは章ごとに、教材データやゲームなどではステージごとにユーザの配信要求に応じて配信する場合、複数回に分けて行なう配信に起因して、コンテンツデータの一括管理が難しくなるという問題が発生する。

【0018】そこで、本発明は、かかる問題を解決するためになされたものであり、その目的は、複数の領域に分離された暗号化コンテンツデータと、複数の領域に含まれる暗号化データを復号および再生するための複数のライセンスとを配信するコンテンツ提供方法を提供することである。

【0019】また、本発明の別の目的は、複数の領域に分離された暗号化コンテンツデータを複数のライセンスによって再生可能なデータ再生装置を提供することである。

【0020】さらに、本発明の別の目的は、複数の領域に分離された暗号化コンテンツデータと複数のライセンスとを記録したデータ記録装置を提供することである。

【0021】

【課題を解決するための手段】この発明によれば、コンテンツ提供方法は、コンテンツデータを暗号化した暗号化コンテンツデータの取得要求を受信する第1のステップと、第1のステップにおいて受信した取得要求に応じて、暗号化コンテンツデータを提供する第2のステップと、暗号化コンテンツデータの一部に対応し、かつ、一部を復号するための第1のライセンスの提供要求を受信する第3のステップと、第3のステップにおいて受信した提供要求に応じて、第1のライセンスを提供する第4のステップと、第1のライセンスと異なり、かつ、暗号化コンテンツデータの第1のライセンスに対応しない他の一部に対応し、他の一部を復号するための第2のライセンスの提供要求を受信する第5のステップと、第5のステップにおいて受信した提供要求に応じて、第2のライセンスを提供する第6のステップと、第2のライセンスの提供に対して課金処理を行なう第7のステップとを含む。

【0022】好ましくは、暗号化コンテンツデータ、第1のライセンス、および第2のライセンスが同じサーバから配信される。

【0023】好ましくは、暗号化コンテンツデータ、および第1のライセンスが第1のサーバから配信され、第2のライセンスが第1のサーバと異なる第2のサーバから配信される。

【0024】好ましくは、暗号化コンテンツデータ、および第1のライセンスは、記録媒体を介して第1のサーバに供給される。

【0025】好ましくは、暗号化コンテンツデータが第1のサーバから提供され、第1および第2のライセンスが第1のサーバと異なる第2のサーバから配信される。

【0026】好ましくは、暗号化コンテンツデータは、記録媒体を介して第1のサーバに供給される。

【0027】好ましくは、第3のステップにおいて、提供要求とともに認証データを受信し、認証データが認証されると第1のライセンスを提供し、第5のステップにおいて、提供要求とともに認証データを受信し、認証データが認証されると第2のライセンスを提供する。

【0028】また、この発明によれば、データ再生装置は、複数のブロックから成る暗号化コンテンツデータを複数のブロックに対応する複数のライセンスによって復号して再生するデータ再生装置であって、暗号化コンテンツデータ、および複数のライセンスが記録されたデータ記録装置とのやり取りを行なうインタフェースと、指示を入力するための操作部と、暗号化コンテンツデータを複数のライセンスによって復号して再生するコンテンツ再生部と、制御部とを備え、制御部は、コンテンツ再

生部において、暗号化コンテンツデータを構成するn番目(nは自然数)のブロックに含まれる暗号化データがn番目のブロックに対応するn番目のライセンスによって復号および再生されているときに、n+1番目のライセンスをインタフェースを介してデータ記録装置から取得してコンテンツ再生部に与える。

【0029】好ましくは、コンテンツ再生部は、n番目のライセンスに含まれるn番目のライセンス鍵を保持する第1のライセンス鍵保持部と、n+1番目のライセンスに含まれるn+1番目のライセンス鍵を保持する第2のライセンス鍵保持部と、第1および第2のライセンス鍵保持部からn番目のライセンス鍵とn+1番目のライセンス鍵とを選択的に取得し、その取得したライセンス鍵によって対応する暗号化データを復号する復号部と、復号部によって復号されたコンテンツデータを再生する再生部とを含む。

【0030】好ましくは、制御部は、鍵変更情報をインタフェースを介してデータ記録装置から取得し、鍵変更情報に基づいてn番目のライセンス鍵とn+1番目のライセンス鍵とを選択して復号部に与える。

【0031】好ましくは、データ記録装置から複数のライセンスの各々を取得するセッションにおいて、異なるセッションキーを発生するセッションキー発生部と、セッションキー発生部によって発生されたセッションキーを受け、そのセッションキーによって暗号化ライセンス鍵を復号し、その復号したライセンス鍵を第1または第2のライセンス鍵保持部に与えるライセンス鍵復号部とをさらに備え、制御部は、セッションキー発生部によって発生されたセッションキーをインタフェースを介してデータ記録装置に入力し、セッションキーによって暗号化された暗号化ライセンス鍵をインタフェースを介してデータ記録装置から取得してライセンス鍵復号部に与える。

【0032】好ましくは、データ再生装置は、ライセンス鍵を提供するライセンス配信サーバからライセンス鍵をダウンロードするための通信を行なうデータ送受信部をさらに備え、制御部は、暗号化コンテンツデータの全部を再生するために必要なライセンスがデータ記録装置に記録されていないとき、データ記録装置に格納されている暗号化コンテンツデータに対応する複数のライセンスによって再生可能なブロックのみを暗号化コンテンツデータの再生順に従って、データ記録装置から取得してコンテンツ再生部に与え、操作部から入力される新たなライセンス鍵の取得指示に従ってライセンス配信サーバから暗号化コンテンツデータを構成するブロックに対応するライセンス鍵をデータ送受信部を介して受信し、その受信したライセンス鍵をデータ記録装置に記録する。

【0033】また、この発明によれば、データ記録装置は、複数のブロックから成る暗号化コンテンツデータおよび複数のブロックに含まれる複数の暗号化データを復

号するための複数のライセンスとを記録するデータ記録装置であって、複数のライセンスを格納するライセンス領域と、暗号化コンテンツデータと、複数のライセンスの各々と暗号化コンテンツデータを構成する複数のブロックとの対応を示すライセンス対応情報とを格納するデータ領域とを備える。

【0034】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【0035】図1は、本発明によるデータ記録装置が暗号化コンテンツデータを取得するデータ配信システムの全体構成を概念的に説明するための概略図である。

【0036】なお、以下では携帯電話網を介してデジタル音楽データをユーザの携帯電話機に装着されたメモリカード110に、またはインターネットを介してデジタル音楽データをカードライタに装着されたメモリカード110に配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画データ等を配信する場合においても適用することが可能なものである。

【0037】図1を参照して、配信キャリア20は、自己の携帯電話網を通じて得たユーザからの配信要求

(配信リクエスト)を配信サーバ10に中継する。著作権の存在する音楽データを管理する配信サーバ10は、データ配信を求めてアクセスして来た携帯電話ユーザの携帯電話機100に装着されたメモリカード110が正当な認証データを持つか否か、すなわち、コンテンツ保護機能を備えた正規のメモリカードであるか否かの認証処理を行ない、正規のメモリカードに対して暗号化コンテンツデータを復号するためのライセンスを配信する配信キャリア20である携帯電話会社に、このような暗号化コンテンツデータおよびライセンスを与える。

【0038】配信キャリア20は、自己の携帯電話網を通じて配信要求を送信した携帯電話機100に装着されたメモリカード110に対して、携帯電話網および携帯電話機100を介して暗号化コンテンツデータとライセンスとを配信する。

【0039】図1においては、たとえば携帯電話ユーザの携帯電話機100には、着脱可能なメモリカード110が装着される構成となっている。メモリカード110は、携帯電話機100により受信された暗号化コンテンツデータを受取り、上記配信にあたって行なわれた暗号化を復号した上で、携帯電話機100中の音楽再生部(図示せず)に与える。

【0040】さらに、たとえば携帯電話ユーザは、携帯電話機100に接続したヘッドホン130等を介してこのようなコンテンツデータを「再生」して、聴取する

ことが可能である。

【0041】このような構成とすることで、まず、メモリカード110を利用しないと、配信サーバ10からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

【0042】しかも、配信キャリア20において、たとえば1曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア20が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【0043】図1に示すデータ配信システムにおいては、暗号化コンテンツデータ {Dc} Kcは、ライセンス鍵Kc1にて復号可能な暗号化を施された領域である試聴領域 {Dc1} Kc1と、ライセンス鍵Kc2にて暗号化を施された本体領域 {Dc2} Kc2とから成り、一つの暗号化コンテンツデータとして構成されている。したがって、試聴には、ライセンス鍵Kc1を含む試聴用ライセンスが必要であり、コンテンツ全体の再生には、試聴用ライセンスとライセンス鍵Kc2を含む本体用ライセンスとが必要である。

【0044】配信サーバ10は、まず、携帯電話網を介して、暗号化コンテンツデータ {Dc} Kcと、ライセンス鍵Kc1を含む試聴用ライセンスを携帯電話機100へ配信する。そして、ユーザは、携帯電話機100に備えられたコンテンツ再生回路（図示せず）において、暗号化コンテンツデータ {Dc} Kcの一部である試聴領域 {Dc1} Kc1が試聴用ライセンスのライセンス鍵Kc1によって復号され、再生された音楽を聴き、このコンテンツをダウンロードしたいと思うと、再度、配信サーバ10に対して本体用ライセンスの配信要求を送信する。そして、配信サーバ10は、受信した配信要求に応じてライセンス鍵Kc2を含む本体用ライセンスを携帯電話網を介して携帯電話機100に配信する。

【0045】そうすると、携帯電話機100のコンテンツ再生回路は、試聴用ライセンスに含まれるライセンス鍵Kc1と本体用ライセンスに含まれるライセンス鍵Kc2を用いて暗号化コンテンツデータ {Dc} Kcの全てを再生できるようになる。

【0046】また、図1においては、配信サーバ10は、暗号化コンテンツデータ {Dc} Kc、およびライセンス鍵Kc1を含む試聴用ライセンスをインターネット網30を介してパーソナルコンピュータ50に配信する。そして、パーソナルコンピュータ50は、USB（Universal Serial Bus）ケーブル70およびカードライタ80を介して暗号化音楽データ {Dc} Kcおよびライセンス鍵Kc1を含む試聴用ライセンスの配信要求を受け、カードライタ80に装着されたメモリカード110の正当性を上述したのと同じ

方法によって判断し、正規なメモリカードに暗号化音楽データ {Dc} Kcおよびライセンス鍵Kc1を含む試聴用ライセンスを記録する。そして、メモリカード110は、カードライタ80から抜かれ、携帯電話機100に装着される。携帯電話機100のユーザは、装着されたメモリカード110から暗号化音楽データ {Dc} Kcおよびライセンス鍵Kc1を読み出し、暗号化音楽データ {Dc} Kcの一部であるライセンス鍵Kc1によって復号可能な領域 {Dc1} Kc1を復号および再生して試聴する。そして、ユーザは、暗号化音楽データ {Dc} Kcの全てを再生するためにライセンス鍵Kc2を含む本体用ライセンスのダウンロードを希望するとき、携帯電話網30を介して配信サーバ10へライセンス鍵Kc2を含む本体用ライセンスの配信要求を送信する。そうすると、配信サーバ10は、再び、メモリカード110が正規のメモリカードであることを確認した上でライセンス鍵Kc2を含む本体用ライセンスを携帯電話網を介して携帯電話機100へ配信する。そして、携帯電話機100は、受信したライセンス鍵Kc2を含む本体用ライセンスをメモリカード110に記録する。ユーザは、携帯電話機100を用いてメモリカード110に記録された暗号化音楽データ {Dc} Kcの全体はライセンス鍵Kc1およびライセンス鍵Kc2を用いて復号して再生する。

【0047】CD-ROM60は、暗号化コンテンツデータ {Dc} Kcと、暗号化コンテンツデータ {Dc} Kcの試聴領域 {Dc1} Kc1を復号するためのライセンス鍵Kc1を含む試聴用ライセンスとが記録されている。パーソナルコンピュータ50は、CD-ROM60から暗号化コンテンツデータ {Dc} Kcと、試聴用ライセンスとを読み出す。そして、パーソナルコンピュータ50は、カードライタ80に装着されたメモリカード110の正当性をカードライタ80およびUSBケーブル70を介して確認し、正規なメモリカードにライセンス鍵Kc1を含む試聴用ライセンスを記録する。そして、メモリカード110は、カードライタ80から抜かれ、携帯電話機100に装着される。携帯電話機100のユーザは、装着されたメモリカード110から暗号化音楽データ {Dc} Kcの一部である試聴領域 {Dc1} Kc1およびライセンス鍵Kc1を読み出し、暗号化音楽データ {Dc} Kcの一部を復号および再生して試聴する。そして、ユーザは、ライセンス鍵Kc2を含む本体用ライセンスのダウンロードを希望するとき、携帯電話網30を介して配信サーバ10へライセンス鍵Kc2を含む本体用ライセンスの配信要求を送信する。

【0048】そうすると、配信サーバ10は、メモリカード110が正規のメモリカードであることを確認した上でライセンス鍵Kc2を含む本体用ライセンスを携帯電話網を介して携帯電話機100へ配信する。そして、携帯電話機100は受信したライセンス鍵Kc2をメモ

リカード 110 に記録する。ユーザは、携帯電話機 100 を用いてメモリカード 110 に記録された暗号化音楽データ {Dc} Kc、ライセンス鍵 Kc1 およびライセンス鍵 Kc2 を読出して暗号化コンテンツデータ {Dc} Kc の全てを再生する。

【0049】この時、CD-ROM 60 に記録されている試験用ライセンスは暗号化された上で記録され、メモリカード 110 にライセンスを記録するための専用プログラムによってのみアクセスできるようになっている必要がある。CD-ROM 60 上のライセンスをそのまま複製しても暗号化コンテンツデータ {Dc} Kc の再生に用いることができない。

【0050】また、CD-ROM 60 は、暗号化音楽データ {Dc} Kc のみが記録されている。パーソナルコンピュータ 50 は、CD-ROM 60 から暗号化音楽データ {Dc} Kc を読出す。そして、パーソナルコンピュータ 50 は、カードライタ 80 および U.S.B ケーブル 70 を介して暗号化音楽データ {Dc} Kc をメモリカード 110 に記録する。そして、メモリカード 110 は、カードライタ 80 から抜かれ、携帯電話機 100 に装着される。携帯電話機 100 のユーザは、装着されたメモリカード 110 に記録された暗号化音楽データ {Dc} Kc に対する試験用ライセンスの配信を携帯電話機網および配信キャリア 20 を介して配信サーバ 10 へ要求する。

【0051】図 1 に示すデータ配信システムにおいては、暗号化コンテンツデータ {Dc} Kc は、ライセンス鍵 Kc1 にて復号可能な暗号化を施された領域である試験領域 {Dc1} Kc1 と、ライセンス鍵 Kc2 にて暗号化を施された本体領域 {Dc2} Kc2 とから成り、一つの暗号化コンテンツデータとして構成されている。したがって、試験には、ライセンス鍵 Kc1 を含む試験用ライセンスが必要であり、コンテンツ全体の再生には、試験用ライセンスと、ライセンス鍵 Kc2 を含む本体用ライセンスとが必要となる。

【0052】配信サーバ 10 は、まず、携帯電話網を介して、暗号化コンテンツデータ {Dc} Kc と、ライセンス鍵 Kc1 を含む試験用ライセンスを携帯電話機 100 へ配信する。そして、ユーザは、携帯電話機 100 に備えられたコンテンツ再生回路（図示せず）において、暗号化コンテンツデータ {Dc} Kc の一部である試験用領域 {Dc1} Kc1 が試験用ライセンスのライセンス鍵 Kc1 によって復号され、かつ、再生された音楽を聴き、このコンテンツをダウンロードしたいと思うと、再度、配信サーバ 10 に対して本体用ライセンスの配信要求を送信する。そして、配信サーバ 10 は、受信した配信要求に応じてライセンス鍵 Kc2 を含む本体用ライセンスを携帯電話網を介して携帯電話機 100 に配信する。

【0053】そうすると、携帯電話機 100 のコンテン

ツ再生回路は、試験用ライセンスに含まれるライセンス鍵 Kc1 と本体用ライセンスに含まれる Kc2 を用いて暗号化コンテンツデータ {Dc} Kc のすべてを再生できるようにする。

【0054】また、説明は省略するが、試験用ライセンスと同様に本体用ライセンスもパーソナルコンピュータ 50 がインターネット網 30 を介して取得してメモリカード 110 に記録させることもできる。インターネット網 30 を介してパーソナルコンピュータ 50 に試験用ライセンスまたは本体用ライセンスを配信する場合は、暗号通信を用いる。

【0055】このように、メモリカード 110 は、各種の方法によって暗号化音楽データ {Dc} Kc、ライセンス鍵 Kc1 を含む試験用ライセンスおよびライセンス鍵 Kc2 を含む本体用ライセンスを取得する。

【0056】図 1 に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話機のユーザ側で再生可能とするためにシステム上必要とされるのは、第 1 には、通信におけるライセンス鍵を配信するための方式であり、さらに第 2 には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第 3 には、このように配信されたコンテンツデータの無断コピーを防止するためのコンテンツデータ保護を実現する構成である。

【0057】本発明の実施の形態においては、特に、配信、および再生の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られた記録装置およびデータ再生端末（コンテンツを再生できるデータ再生端末を携帯電話機とも言う。以下同じ）に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

【0058】なお、以下の説明においては、配信サーバ 10 から各携帯電話機を介してメモリカードへ、またはパーソナルコンピュータからカードライタを介してメモリカードへコンテンツデータ（暗号化コンテンツデータおよびライセンス）を伝送する処理を「配信」と称することとする。

【0059】図 2 は、図 1 に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

【0060】まず、配信サーバ 10 より配信されるデータについて説明する。Dc は、音楽データ等のコンテンツデータである。コンテンツデータ Dc は、ライセンス鍵 Kc で復号可能な暗号化が施される。コンテンツデータ Dc は、試験領域 Dc1 と本体領域 Dc2 とから成り、それぞれ、異なる暗号鍵によって暗号化されている。試験領域 Dc1 は、ライセンス鍵 Kc1 によって復号可能な暗号化が施された試験領域 {Dc1} Kc1 と

して、また、本体領域 D c 2 は、ライセンス鍵 K c 2 によって復号可能な暗号化が施された本体領域 { D c 2 } K c 2 として 1 つの暗号化コンテンツデータ { D c } K c を構成する。コンテンツデータ D c は、必ず、暗号化された暗号化コンテンツデータ { D c } K c として携帯電話機 100 またはパーソナルコンピュータ 50 へ配信される。その結果、全体としては、コンテンツデータ D c は、ライセンス鍵 K c (K c 1 と K c 2 とから成る) によって復号可能な暗号化が施された暗号化コンテンツデータ { D c } K c として配信サーバ 10 より携帯電話機 100 またはパーソナルコンピュータ 50 のユーザに配布される。

【0061】なお、以下においては、{ Y } X という表記は、データ Y を、復号鍵 X により復号可能な暗号化を施したことを示すものとする。

【0062】図 3 を参照して、情報データベース 304 が保持する暗号化コンテンツデータ { D c } K c のフォーマットについて説明する。暗号化コンテンツデータ { D c } K c が暗号化音楽データであるとき、暗号化コンテンツデータ { D c } K c は図 3 の (a) に示すフォーマットから成る。暗号化音楽データ 90 は、試聴領域 91 ({ D c 1 } K c 1) と本体領域 92 ({ D c 2 } K c 2) とから成る。試聴領域 91 ({ D c 1 } K c 1) は、ライセンス鍵 K c 1 によって復号可能である。本体領域 92 ({ D c 2 } K c 2) は、ライセンス鍵 K c 2 によって復号可能である。試聴領域 91 ({ D c 1 } K c 1) は、暗号化コンテンツデータ { D c } K c の途中に含まれ、本体領域 92 ({ D c 2 } K c 2) が 2 分割されている。この場合、試聴用の暗号化音楽データ 91 は、曲のサビから成る。試聴領域 91 ({ D c 1 } K c 1) は、1 つの連続する領域として示したが、本体領域 92 ({ D c 2 } K c 2) と同様に、本体領域 92 ({ D c 2 } K c 2) によって分割された領域であってもよい。

【0063】また、暗号化コンテンツデータ { D c } K c は、図 3 の (b) に示すフォーマットから成ってもよい。暗号化音楽データ 93 は、試聴用の暗号化音楽データ 94 と本体用の暗号化音楽データ 95 とから成る。試聴用の暗号化音楽データ 94 は、ライセンス鍵 K c 1 によって復号可能である。本体用の暗号化音楽データ 95 は、ライセンス鍵 K c 2 によって復号可能である。試聴用の暗号化音楽データ 94 は、暗号化コンテンツデータ { D c } K c の最初に含まれている。この場合、試聴用の暗号化音楽データ 94 は、曲のイントロから成る。

【0064】図 4 を参照して、暗号化コンテンツデータ { D c } K c 84 の生成について説明する。平文のコンテンツデータである源データ D c 81 を最小暗号化単位である M バイトの固定長を有するブロック B L K 1, B L K 2, . . . , B L K k に分割してブロックデータ 8

2 を生成する (k は自然数)。最終ブロック B L K k が M バイトに満たないときは、意味を持たないダミーデータをデータ末尾に追加して M バイトのブロックを構成する (斜線部)。そして、ブロック B L K 1, B L K 2, . . . , B L K k の各々を個々に暗号化して暗号化データ 83 を生成する。このとき、ブロックごとにライセンス鍵 K c 1, K c 2 のいずれに対応させるかが決定される。ライセンス鍵とブロックとの対応は付加情報 D c - i n f 内にライセンス鍵対応情報として記録される。その後、ブロック B L K 1, B L K 2, . . . , B L K k の各々にヘッダを追加して暗号化コンテンツデータ { D c } K c 84 を生成する。すなわち、ブロック B L K 1 は、ヘッダ 841 と、暗号化データ 842 とから成り、ブロック B L K 2 は、ヘッダ 843 と暗号化データ 844 とから成り、ブロック B L K k は、ヘッダ 845 と暗号化データ 846 とから成る。ヘッダ 841, 843, 845 は、N バイトのデータであり、そのブロックが暗号化ブロックであるか非暗号化ブロックであることを示すスクランブルフラグが記録されている。つまり、ヘッダ 841, 843, 845 は、暗号化ブロックであることを示す「1」または非暗号化ブロックであることを示す「0」を含む。したがって、図 3 の示す暗号化コンテンツデータは、図 4 に示すデータフォーマットから成り、試聴領域および本体領域は重複しない複数のブロックによって構成される。

【0065】再び、図 2 を参照して、配信サーバ 10 からは、暗号化コンテンツデータとともに、暗号化コンテンツデータに対するライセンス鍵対応情報、コンテンツデータの著作権に関する情報あるいはサーバアクセス関連情報等の平文情報としての付加情報 D c - i n f が配布される。また、ライセンスとして、ライセンス鍵 K c、配信サーバ 10 からのライセンス鍵等を特定するための管理コードであるライセンス I D が配信サーバ 10 と、携帯電話機 100 またはパーソナルコンピュータ 50 との間でやり取りされ、かつ、メモリカード 110 にライセンス鍵 K c i とともに記録される。さらに、ライセンスとしては、コンテンツデータ D c を識別するためのコードであるコンテンツ I D や、利用者側からの指定によって決定されるライセンスの種類や機能限定等の情報を含んだライセンス購入条件 A C に基づいて生成される、記録装置 (メモリカード) におけるライセンスのアクセスに対する制限に関する情報であるアクセス制御情報 A C m およびデータ再生端末における再生に関する制御情報である再生制御情報 A C p 等が存在する。具体的には、アクセス制御情報 A C m はメモリカードからのライセンスまたはライセンス鍵を外部に出力するに当たっての制御情報であり、再生可能回数 (再生のためにライセンス鍵を出力する数)、およびライセンスの移動・複製に関する制限情報などがある。再生制御情報 A C p は、再生するためにコンテンツ再生回路がライセンス鍵を受

取った後に、再生を制限する情報であり、再生期限、再生速度変更制限、再生範囲指定（部分ライセンス）などがある。

【0066】以後、コンテンツIDとライセンス鍵Kci (i=1, 2) とライセンスIDとアクセス制御情報ACmと再生制御情報ACpとを併せて、ライセンスと総称することとする。ライセンス鍵Kc1を含むライセンスが試験用ライセンスであり、ライセンス鍵Kc2を含むライセンスが本体用ライセンスである。

【0067】また、以降では、簡単化のためアクセス制御情報ACmは再生回数の制限を行なう制御情報である再生回数(0:再生不可、1~254:再生可能回数、255:制限無し)、ライセンスの移動および複製を制限する移動・複製フラグ(1:移動複製不可、2:移動のみ可、3:移動複製禁止)の2項目とし、再生制御情報ACpは再生可能な期限を規定する制御情報である再生期限(UTCtimeコード)のみを制限するものとする。

【0068】図5は、図1に示すデータ配信システムにおいて使用される認証のためのデータ、情報等の特性を説明する図である。

【0069】コンテンツ再生回路、およびメモリカードには固有の公開暗号鍵KppyおよびKpmwがそれぞれ設けられ、公開暗号鍵KppyおよびKpmwはコンテンツ再生回路に固有の秘密復号鍵Kpyおよびメモリカードに固有の秘密復号鍵Kmwによってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、コンテンツ再生回路、およびメモリカードの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称し、これらの公開暗号鍵をクラス公開暗号鍵、秘密復号鍵をクラス秘密復号鍵、クラス鍵を共有する単位をクラスと称する。クラスは、製造会社や製品の種類、製造時のロット等によって異なる。

【0070】また、コンテンツ再生回路（携帯電話機、再生端末）のクラス証明書としてCpyが設けられ、メモリカードのクラス証明書としてCmwが設けられる。これらのクラス証明書は、コンテンツ再生回路、およびメモリカードのクラスごとに異なる情報を有する。耐タンパモジュールが破られたり、クラス鍵による暗号が破られた、すなわち、秘密復号鍵が漏洩したクラスに対しては、禁止クラスリストにリストアップされてライセンス取得の禁止対象となる。

【0071】これらのコンテンツ再生回路のクラス公開暗号鍵およびクラス証明書は、認証データ{Kppy/Cpy}KPaの形式で、メモリカードのクラス公開暗号鍵およびクラス証明書は認証データ{Kpmw/Cmw}KPaの形式で、出荷時にデータ再生回路、およびメモリカードにそれぞれ記録される。後ほど詳細に説明するが、KPaは配信システム全体で共通の公開認証鍵である。

【0072】また、メモリカード110内のデータ処理を管理するための鍵として、メモリカードという媒体ごとに設定される公開暗号鍵Kpmcxと、公開暗号鍵Kpmcxで暗号化されたデータを復号することが可能なそれぞれに固有の秘密復号鍵Kmcxが存在する。このメモリカードごとに個別な公開暗号鍵および秘密復号鍵を総称して個別鍵と称し、公開暗号鍵Kpmcxを個別公開暗号鍵、秘密復号鍵Kmcxを個別秘密復号鍵と称する。

【0073】メモリカード外とメモリカード間でのデータ授受でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、および再生が行なわれるごとに配信サーバ10、携帯電話機100、およびメモリカード110において生成される共通鍵Ks1~Ks3が用いられる。

【0074】ここで、共通鍵Ks1~Ks3は、配信サーバ、コンテンツ再生回路もしくはメモリカード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵Ks1~Ks3を「セッションキー」とも呼ぶこととする。

【0075】これらのセッションキーKs1~Ks3は、各セッションごとに固有の値を有することにより、配信サーバ、コンテンツ再生回路、およびメモリカードによって管理される。具体的には、セッションキーKs1は、配信サーバによって配信セッションごとに発生される。セッションキーKs2は、メモリカードによって配信セッションおよび再生セッションごとに発生し、セッションキーKs3は、コンテンツ再生回路において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行した上でライセンス鍵等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【0076】なお、カードライター80とUSBケーブル70を介してパーソナルコンピュータ50とメモリカード110との間の通信においては、配信サーバ10と携帯電話機100の機能をパーソナルコンピュータ50に読替え、メモリカードインタフェース1200をカードライター80およびUSBケーブル70に読替えればよい。

【0077】図6は、図1に示した配信サーバ10の構成を示す概略ブロック図である。配信サーバ10は、コンテンツデータを所定の方式に従って暗号化したデータやコンテンツID等の配信情報を保持するための情報データベース304と、携帯電話機の各ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース302と、情報データベース304に保持されたコンテンツデータのメニューを保

持するメニューデータベース 3 0 7 と、ライセンスの配信ごとにコンテンツデータおよびライセンス鍵等の配信を特定するトランザクション ID 等の配信に関するログを保持する配信記録データベース 3 0 8 と、情報データベース 3 0 4、課金データベース 3 0 2、メニューデータベース 3 0 7、および配信記録データベース 3 0 8 からのデータをバス B S 1 を介して受取り、所定の処理を行なうためのデータ処理部 3 1 0 と、通信網を介して、配信キャリア 2 0 とデータ処理部 3 1 0 との間でデータ授受を行なうための通信装置 3 5 0 とを備える。

【0078】暗号化コンテンツデータ {Dc} Kc が朗読データ、教材データ、またはゲームソフトのデータであるとき、暗号化コンテンツデータ {Dc} Kc は、図 1 3 の (c) に示すフォーマットから成る。暗号化コンテンツデータ 9 6 は、複数の領域 9 6 1 ~ 9 6 7 から成る。各領域 9 6 1 ~ 9 6 7 は、それぞれ、ライセンス鍵 Kc 1、Kc 2、Kc 3、Kc 4、Kc 5、Kc 6、Kc 7 によって復号可能である。

【0079】暗号化コンテンツデータ {Dc} Kc が既に説明した音楽データと同様に試しようの領域を備えたビデオデータであるとき、暗号化コンテンツデータ {Dc} Kc は、図 1 3 の (d) に示すフォーマットから成る。暗号化データ 9 7 は、付属用の領域 9 7 1 と本体用の領域 9 7 2 とから成る。付属用の領域 9 7 1 は、ライセンス鍵 Kc 1 によって復号可能である。本体用の領域 9 7 2 は、ライセンス鍵 Kc 2 によって復号可能である。付属用の領域 9 7 1 は、ビデオまたはゲームのサブタイトルから成る。暗号化コンテンツデータ 9 6、9 7 の復号については、図 7 に示すコンテンツ再生回路 1 5 5 0 が受理可能である。この場合、音楽再生部 1 5 2 0 が各コンテンツに適合した再生回路に置換えられる。

【0080】データ処理部 3 1 0 は、バス B S 1 上のデータに応じて、データ処理部 3 1 0 の動作を制御するための配信制御部 3 1 5 と、配信制御部 3 1 5 に制御されて、配信セッション時にセッションキー Ks 1 を発生するためのセッションキー発生部 3 1 6 と、メモリカードから送られてきた認証のための認証データ {K P m w / C m w} K P a を復号するための 2 種類の公開認証鍵 K P a を保持する認証鍵保持部 3 1 3 と、メモリカードから送られてきた認証のための認証データ {K P m w / C m w} K P a を通信装置 3 5 0 およびバス B S 1 を介して受けて、認証鍵保持部 3 1 3 からの公開認証鍵 K P a によって復号処理を行なう復号処理部 3 1 2 と、配信セッションごとに、セッション鍵 Ks 1 を発生するセッションキー発生部 3 1 6、セッションキー発生部 3 1 6 より生成されたセッションキー Ks 1 を復号処理部 3 1 2 によって得られたクラス公開暗号鍵 K P m w を用いて暗号化して、バス B S 1 に出力するための暗号化処理部 3 1 8 と、セッションキー Ks 1 によって暗号化された上で送信されたデータをバス B S 1 より受けて、復号

処理を行なう復号処理部 3 2 0 とを含む。

【0081】データ処理部 3 1 0 は、さらに、配信制御部 3 1 5 から与えられるライセンス鍵 Kc およびアクセス制御情報 A C m を、復号処理部 3 2 0 によって得られたメモリカードごとに個別公開暗号鍵 K P m c x によって暗号化するための暗号化処理部 3 2 6 と、暗号化処理部 3 2 6 の出力を、復号処理部 3 2 0 から与えられるセッションキー Ks 2 によってさらに暗号化してバス B S 1 に出力するための暗号化処理部 3 2 8 とを含む。

10 【0082】配信サーバ 1 0 の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0083】図 7 は、図 1 に示した携帯電話機 1 0 0 の構成を説明するための概略ブロック図である。

【0084】携帯電話機 1 0 0 は、携帯電話機 1 0 0 の各部のデータ授受を行なうためのバス B S 2 と、携帯電話網により無線伝送される信号を受信するためのアンテナ 1 1 0 1 と、アンテナからの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ 1 1 0 1 に与えるための送受信部 1 1 0 2 とを含む。

【0085】携帯電話機 1 0 0 は、さらに、携帯電話機 1 0 0 のユーザの音声データを取込むためのマイク 1 1 0 3 と、マイク 1 1 0 3 からの音声データをアナログ信号からデジタル信号に変換する A D 変換器 1 1 0 4 と、A D 変換器 1 1 0 4 からの音声データを所定の方式に変調する音声符号化部 1 1 0 5 とを含む。

【0086】携帯電話機 1 0 0 は、さらに、アンテナ 1 1 0 1 および送受信部 1 1 0 2 を介して受信した他の携帯電話機のユーザの音声データを再生する音声再生部 1 1 0 6 と、音声再生部 1 1 0 6 からのデータをデジタル信号からアナログ信号へ変換する D A 変換器 1 1 0 7 と、D A 変換器 1 1 0 7 からの音声データを外部へ出力するスピーカ 1 1 0 8 とを含む。

【0087】携帯電話機 1 0 0 は、さらに、バス B S 2 を介して携帯電話機 1 0 0 の動作を制御するためのコントローラ 1 1 0 9 と、外部からの指示を携帯電話機 1 0 0 に与えるための操作パネル 1 1 1 1 と、コントローラ 1 1 0 9 等から出力される情報をユーザに視覚情報として与えるための表示パネル 1 1 1 0 とを含む。

【0088】携帯電話機 1 0 0 は、さらに、配信サーバ 1 0 からのコンテンツデータ（音楽データ）を記憶し、かつ、復号処理を行なうための着脱可能なメモリカード 1 1 1 0 と、メモリカード 1 1 1 0 とバス B S 2 との間のデータの授受を制御するためのメモリカードインタフェース 1 2 0 0 とを含む。

【0089】携帯電話機 1 0 0 は、さらに、クラス公開暗号鍵 K P p 1 およびクラス証明書 C p 1 を公開認証鍵 K P a で復号することでその正当性を認証できる状態に暗号化した認証データ {K P p 1 / C p 1} K P a を

保持する認証データ保持部1500を含む。ここで、再生端末102のクラスyは、y=1であるとする。

【0090】携帯電話機100は、さらに、クラス固有の復号鍵であるKp1を保持するKp1保持部1502と、バスBS2から受けたデータをKp1によって復号し、メモリカード110によって発生されたセッションキーKs2を得る復号処理部1504とを含む。

【0091】携帯電話機100は、さらに、メモリカード110に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード110との間でバスBS2上においてやり取りされるデータを暗号化するためのセッションキーKs3を乱数等により発生するセッションキー発生部1508と、暗号化コンテンツデータの再生セッションにおいてメモリカード110からライセンス鍵Kc(Kc1とKc2とから成る。以下同じ)および再生制御情報ACpを受取る際に、セッションキー発生部1508により発生されたセッションキーKs3を復号処理部1504によって得られたセッションキーKs2によって暗号化し、バスBS2に出力する暗号化処理部1506とを含む。

【0092】携帯電話機100は、さらに、バスBS2上のデータをセッションキーKs3によって復号して、ライセンス鍵Kcおよび再生制御情報ACpを出力する復号処理部1510と、コントローラ1109からの指示によって復号処理部1510から出力されたライセンス鍵Kc1、Kc2のいずれか一方を端子1512を介してKc保持部1514へ出力し、端子1513を介してライセンス鍵Kc1、Kc2のいずれか他方をKc保持部1515へ出力するスイッチ1511とを含む。

【0093】携帯電話機100は、さらに、端子1512から入力されたライセンス鍵Kc1、Kc2のいずれかを保持するKc保持部1514と、端子1513から入力されたKc保持部1514が保持するライセンス鍵とは異なるライセンス鍵、すなわち、Kc保持部1514がライセンス鍵Kc1を保持するときライセンス鍵Kc2を保持するKc保持部1515とを含む。

【0094】携帯電話機100は、さらに、Kc保持部1514またはKc保持部1515に保持される2つのライセンス鍵Kc1、Kc2のいずれか1つを選択して復号処理部1519へ出力するスイッチ1518を含む。スイッチ1518は、Kc保持部1514からのライセンス鍵を受ける端子1516と、Kc保持部1515からのライセンス鍵を受ける端子1517とを含む。なお、スイッチ1518は、コントローラ1109からの指示によって端子1516または端子1517を選択してライセンス鍵Kc1またはライセンス鍵Kc2を復号処理部1519へ出力する。

【0095】携帯電話機100は、さらに、バスBS2より暗号化コンテンツデータ{Dc}Kcを受けて、スイッチ1518から入力されたライセンス鍵Kc1また

はKc2によって暗号化コンテンツデータ{Dc}Kcを復号する復号処理部1519とを含む。試験用ライセンスのみをメモリカード110に記録している場合には、ライセンス鍵Kc1にて復号再生可能な試験領域{Dc1}Kc1のみ再生可能である。

【0096】携帯電話機100は、さらに、復号処理部1519からの出力を受けてコンテンツデータを再生するための音楽再生部1520と、音楽再生部1520の出力をデジタル信号からアナログ信号に変換するDA変換器1521と、DA変換器1521の出力をヘッドホンなどの外部出力装置(図示省略)へ出力するための端子1522とを含む。

【0097】なお、図7においては、点線で囲んだ領域は暗号化コンテンツデータを復号して音楽データを再生するコンテンツ再生回路1550を構成する。

【0098】携帯電話機100の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0099】図8は、図1に示すメモリカード110の構成を説明するための概略ブロック図である。

【0100】既に説明したように、メモリカードのクラス公開暗号鍵およびクラス秘密復号鍵として、KpmwおよびKmwが設けられ、メモリカードのクラス証明書Cmwが設けられるが、メモリカード110においては、自然数w=3で表わされるものとする。また、メモリカードを識別する自然数xはx=4で表されるものとする。

【0101】したがって、メモリカード110は、認証データ{Kpm3//Cm3}Kpaを保持する認証データ保持部1400と、メモリカードごとに設定される固有の復号鍵である個別秘密復号鍵Kmc4を保持するKmc保持部1402と、クラス秘密復号鍵Kmc3を保持するKm保持部1421と、個別秘密復号鍵Kmc4によって復号可能な公開暗号鍵Kpmc4を保持するKpmc保持部1416とを含む。

【0102】このように、メモリカードという記録装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンス鍵の管理をメモリカード単位で実行することが可能になる。

【0103】メモリカード110は、さらに、メモリカードインタフェース1200との間で信号を端子1426を介して授受するインタフェース1424と、インタフェース1424との間で信号をやり取りするバスBS4と、バスBS4にインタフェース1424から与えられるデータから、クラス秘密復号鍵Kmc3をKm保持部1421から受けて、配信サーバ10が配信セッションにおいて生成したセッションキーKs1を接点Paに出力する復号処理部1422と、Kpa保持部1414から公開認証鍵Kpaを受けて、バスBS4に与えられる

データから公開認証鍵 K P a による復号処理を実行して復号結果と得られたクラス証明書をコントローラ 1420 に、得られたクラス公開鍵を暗号化処理部 1410 に出力する復号処理部 1408 と、切換スイッチ 1442 によって選択的に与えられる鍵によって、切換スイッチ 1446 によって選択的に与えられるデータを暗号化してバス B S 4 に出力する暗号化処理部 1406 とを含む。

【0104】メモリカード 110 は、さらに、配信、および再生の各セッションにおいてセッションキー K s 2 を発生するセッションキー発生部 1418 と、セッションキー発生部 1418 の出力したセッションキー K s 2 を復号処理部 1408 によって得られるクラス公開暗号鍵 K P p y もしくは K P m w によって暗号化してバス B S 4 に送出する暗号化処理部 1410 と、バス B S 4 よりセッションキー K s 2 によって暗号化されたデータを受けてセッションキー発生部 1418 より得たセッションキー K s 2 によって復号する復号処理部 1412 と、暗号化コンテンツデータの再生セッションにおいてメモリ 1415 から読出されたライセンス鍵 K c および再生制御情報 A C p を、復号処理部 1412 で復号された他のメモリカード 110 の個別公開暗号鍵 K P m c x (x ≠ 4) で暗号化する暗号化処理部 1417 とを含む。

【0105】メモリカード 110 は、さらに、バス B S 4 上のデータを個別公開暗号鍵 K P m c 4 と対をなすメモリカード 110 の個別秘密復号鍵 K m c 4 によって復号するための復号処理部 1404 と、暗号化コンテンツデータ {D c} K c と、暗号化コンテンツデータ {D c} K c を再生するためのライセンス (K c, A C p, A C m, ライセンス I D, コンテンツ I D) と、付加情報 D c - i n f とをバス B S 4 より受けて格納するためのメモリ 1415 とを含む。メモリ 1415 は、例えば半導体メモリによって構成される。また、メモリ 1415 は、ライセンス領域 1415 A と、データ領域 1415 B とから成る。ライセンス領域 1415 A は、ライセンスを記録するための領域である。データ領域 1415 B は、暗号化コンテンツデータ {D c} K c、および暗号化コンテンツデータの付加情報 D c - i n f を記録するための領域である。なお、データ領域 1415 B は、外部からアクセス可能である。

【0106】メモリカード 110 は、さらに、バス B S 4 を介して外部との間でデータ授受を行ない、バス B S 4 との間で再生情報等を受けて、メモリカード 110 の動作を制御するためのコントローラ 1420 を含む。

【0107】なお、ライセンス領域 1415 A は、耐タンパモジュール領域に構成される。また、ライセンス領域 1415 A とデータ領域 1415 B とは、1つのメモリ 1415 内に構成されている必要はなく、それぞれ、別々に構成されていても良い。さらに、メモリ 1415 は、データ領域 1415 B を伴わないライセンス専用の

領域であってもよい。

【0108】以下、図 1 に示すデータ配信システムにおける各セッションの動作について説明する。

【0109】〔試聴用配信〕図 1 に示す配信サーバ 10 は、携帯電話網を介して携帯電話機 100 に装着されたメモリカード 110 に暗号化音楽データ {D c} K c、ライセンス鍵 K c 1 を含む試聴用ライセンス、およびライセンス鍵 K c 2 を含む本体用ライセンスを配信する動作について説明する。図 9 は、配信サーバ 10 からメモリカード 110 への暗号化音楽データ {D c} K c、ライセンス鍵 K c 1 を含む試聴用ライセンス、およびライセンス K c 1, K c 2 の配信の全体動作を示すフローチャートである。携帯電話機 100 は、携帯電話機 100 のユーザの指示に応じて、携帯電話網を介して配信サーバ 10 へ暗号化音楽データ {D c} K c およびライセンス鍵 K c 1 を含む試聴用ライセンスの配信要求を送信し、配信サーバ 10 から暗号化音楽データ {D c} K c および試聴用ライセンスを受信する。そして、携帯電話機 100 は、受信した暗号化音楽データ {D c} K c およびライセンス鍵 K c 1 を含む試聴用ライセンスをメモリカード 110 に記録する (ステップ S 10)。その後、携帯電話機 100 は、ユーザからの試聴指示に応じて、メモリカード 110 から暗号化音楽データ {D c} K c の一部である試聴領域 {D c 1} K c 1 およびライセンス鍵 K c 1 を読出し、コンテンツ再生回路 1550 において試聴用のライセンスに含まれるライセンス鍵 K c 1 によって復号可能な暗号化音楽データ {D c 1} K c 1 を復号および再生する。そして、ユーザは、再生された音楽データをヘッドホン 130 を介して試聴する (ステップ S 20)。

【0110】ユーザは、試聴した音楽データの購入を希望するとき、ライセンス鍵 K c 2 を含む本体用ライセンスのダウンロード要求を携帯電話機 100 に入力する。そうすると、携帯電話機 100 は、携帯電話網を介してライセンス鍵 K c 2 を含む本体用ライセンスの配信要求を配信サーバ 10 へ送信し、配信サーバ 10 からライセンス鍵 K c 2 を含む本体用ライセンスを受信し、その受信したライセンス鍵 K c 2 を含む本体用ライセンスをメモリカード 110 に記録する (ステップ S 30)。その後、携帯電話機 100 は、ユーザの再生要求に応じて、暗号化音楽データ {D c} K c および 2つのライセンス鍵 K c 1, K c 2 をメモリカード 110 から読出し、コンテンツ再生回路 1550 において暗号化音楽データ {D c} K c を、暗号化コンテンツデータ {D c} K c の各領域に適合したライセンス鍵 K c 1 およびライセンス鍵 K c 2 を用いて復号および再生する。

【0111】以下、ステップ S 10, S 20, S 30 の詳細について説明する。図 10 および図 11 は、図 9 のステップ S 10 およびステップ S 30 におけるライセンスの配信処理の詳細な動作を説明するためのフローチャ

ートである。まず、試験用のライセンスおよび暗号化コンテンツデータ {Dc} Kc を配信サーバ 10 からダウンロードするステップ S 10 の詳細について説明する。

【0112】図 10 における処理以前に、携帯電話機 100 のユーザは、配信サーバ 10 に対して電話網を介して接続し、購入を希望するコンテンツに対するコンテンツ ID を取得し、必要とするライセンスの種類を決定していることを前提としている。また、フローチャートにおけるライセンス鍵 Kci (i=1, 2) は、Kc1 または Kc2 のいずれかのライセンス鍵であり、この場合、ライセンス鍵 Kc1 を含む試験用ライセンスの取得を目的としているため、i=1 である。図 10 および図 11 におけるライセンス鍵 Kci の i を i=1 と読替えて試験用ライセンスの配信を説明する。

【0113】図 10 を参照して、携帯電話機 100 のユーザから操作パネル 1111 を介してコンテンツ ID の指定による配信リクエストがなされる (ステップ S 100)。そして、操作パネル 1111 を介して試験用の暗号化音楽データ {Dc1} Kc1 のライセンス Kc1 を購入するための購入条件 AC が入力される (ステップ S 102)。つまり、選択した暗号化音楽データ {Dc} Kc を復号するライセンス鍵 Kci をダウンロードするための条件として、ライセンス鍵 Kc1 なのか、ライセンス鍵 Kc2 なのか、すなわち試験用ライセンスなのか本体用ライセンスなのかを指示する。さらに、本体用ライセンスの場合には、暗号化コンテンツデータのアクセス制御情報 ACm、および再生制御情報 ACp を設定するための条件がライセンス購入条件 AC として入力される。

【0114】暗号化コンテンツデータの購入条件 AC が入力されると、コントローラ 1109 は、バス BS2 およびメモリカードインタフェース 1200 を介してメモリカード 110 へ認証データの出力指示を与える (ステップ S 104)。メモリカード 110 のコントローラ 1420 は、端子 1426、インタフェース 1424 およびバス BS4 を介して認証データの送信要求を受信する (ステップ S 106)。そして、コントローラ 1420 は、バス BS4 を介して認証データ保持部 1400 から認証データ {Kpm3//Cm3} KPa を読出し、{Kpm3//Cm3} KPa をバス BS4、インタフェース 1424 および端子 1426 を介して出力する (ステップ S 108)。

【0115】携帯電話機 100 のコントローラ 1109 は、メモリカード 110 からの認証データ {Kpm3//Cm3} KPa に加えて、コンテンツ ID、ライセンス購入条件のデータ AC、および配信リクエストを配信サーバ 10 に対して送信する (ステップ S 110)。

【0116】配信サーバ 10 では、携帯電話機 100 から配信リクエスト、コンテンツ ID、認証データ {Kpm3//Cm3} KPa、およびライセンス購入条件の

データ AC を受信し (ステップ S 112)、復号処理部 312 においてメモリカード 110 から出力された認証データを公開認証鍵 KPa で復号処理を実行する (ステップ S 114)。

【0117】配信制御部 315 は、復号処理部 312 における復号処理結果から、正規の機関でその正当性を証明するための暗号化を施した認証データを受信したか否かを判断する認証処理を行なう (ステップ S 116)。正当な認証データであると判断された場合、配信制御部 315 は、クラス公開暗号鍵 Kpm3 およびクラス証明書 Cm3 を承認し、受理する。そして、次の処理 (ステップ S 118) へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵 Kpm3 およびクラス証明書 Cm3 を受理しないで配信セッションを終了する (ステップ S 164)。

【0118】認証の結果、正当な認証データを持つメモリカードを装着した携帯電話機からのアクセスであることが確認されると、配信サーバ 10 において、セッションキー発生部 316 は、配信のためのセッションキー Ks1 を生成する (ステップ S 118)。セッションキー Ks1 は、復号処理部 312 によって得られたメモリカード 110 に対応するクラス公開暗号鍵 Kpm3 によって、暗号化処理部 318 によって暗号化される (ステップ S 120)。

【0119】配信制御部 315 は、ライセンス ID を生成し (ステップ S 122)、ライセンス ID および暗号化されたセッションキー Ks1 は、ライセンス ID // {Ks1} Km3 として、バス BS1 および通信装置 350 を介して外部に出力される (ステップ S 124)。

【0120】携帯電話機 100 が、ライセンス ID // {Ks1} Km3 を受信すると、コントローラ 1109 は、ライセンス ID // {Ks1} Km3 をメモリカード 110 に入力する (ステップ S 126)。そうすると、メモリカード 110 においては、端子 1426 およびインタフェース 1424 を介して、コントローラ 1420 は、ライセンス ID // {Ks1} Km3 を受理する (ステップ S 128)。そして、コントローラ 1420 は、バス BS4 を介して {Ks1} Km3 を復号処理部 1422 へ与え、復号処理部 1422 は、保持部 1421 に保持されるメモリカード 110 に固有なクラス秘密復号鍵 Km3 によって復号処理することにより、セッションキー Ks1 を復号し、セッションキー Ks1 を受理する (ステップ S 132)。

【0121】コントローラ 1420 は、配信サーバ 10 で生成されたセッションキー Ks1 の受理を確認すると、セッションキー発生部 1418 に対してメモリカード 110 において配信動作時に生成されるセッションキー Ks2 の生成を指示する。そして、セッションキー発生部 1418 は、セッションキー Ks2 を生成する (ステップ S 134)。

【0122】暗号化処理部1406は、切換スイッチ1442の接点Paを介して復号処理部1422より与えられるセッションキーKs1によって、切換スイッチ1446の接点を順次切換えることによって与えられるセッションキーKs2、および個別公開暗号鍵KPmc4を1つのデータ列として暗号化して、{Ks2//KPmc4}Ks1をバスBS4に出力する。バスBS4に出力された暗号化データ{Ks2//KPmc4}Ks1は、バスBS4からインタフェース1424および端子1426を介して携帯電話機100に出力され(ステップS138)、携帯電話機100から配信サーバ10に送信される(ステップS140)。

【0123】図11を参照して、配信サーバ10は、{Ks2//KPmc4}Ks1を受信して、復号処理部320においてセッションキーKs1による復号処理を実行し、メモリカード110で生成されたセッションキーKs2、およびメモリカード110に固有の公開暗号鍵KPmc4を受理する(ステップS142)。

【0124】配信制御部315は、ステップS112で取得したコンテンツIDと購入条件ACに従ってライセンス鍵Kc1を情報データベース304から取得し(ステップS144)、ステップS112で取得したライセンス購入条件のデータACに従って、アクセス制御情報ACmおよび再生制御情報ACpを決定する(ステップS146)。

【0125】配信制御部315は、生成したライセンス、すなわち、ライセンスID、コンテンツID、ライセンス鍵Kc、再生制御情報ACp、およびアクセス制御情報ACmを暗号化処理部326に与える。暗号化処理部326は、復号処理部320によって得られたメモリカード110に固有の公開暗号鍵KPmc4によってライセンスを暗号化して暗号化データ{ライセンスID//コンテンツID//Kc1//ACm//ACp}Kmc4を生成する(ステップS148)。そして、暗号化処理部328は、暗号化処理部326からの暗号化データ{ライセンスID//コンテンツID//Kc1//ACm//ACp}Kmc4を、復号処理部320からのセッションキーKs2によって暗号化し、暗号化データ{{ライセンスID//コンテンツID//Kc1//ACm//ACp}Kmc4}Ks2を出力する。配信制御部315は、バスBS1および通信装置350を介して暗号化データ{{ライセンスID//コンテンツID//Kc1//ACm//ACp}Kmc4}Ks2を携帯電話機100へ送信する(ステップS150)。

【0126】携帯電話機100は、送信された暗号化データ{{ライセンスID//コンテンツID//Kc1//ACm//ACp}Kmc4}Ks2を受信し、バスBS2を介してメモリカード110に入力する(ステップS152)。メモリカード110においては、端子

1426およびインタフェース1424を介して、バスBS4に与えられた受信データを復号処理部1412によって復号する。復号処理部1412は、セッションキー発生部1418から与えられたセッションキーKs2を用いてバスBS4の受信データを復号し、バスBS4に出力する(ステップS154)。

【0127】この段階で、バスBS4には、Kmc保持部1402に保持される秘密復号鍵Kmc4で復号可能な暗号化ライセンス{ライセンスID//コンテンツID//Kc1//ACm//ACp}Kmc4が出力される(ステップS154)。

【0128】コントローラ1420の指示によって、暗号化ライセンス{ライセンスID//コンテンツID//Kc1//ACm//ACp}Kmc4は、復号処理部1404において、個別秘密復号鍵Kmc4によって復号され、ライセンス(ライセンス鍵Kc1、ライセンスID、コンテンツID、アクセス制御情報ACmおよび再生制御情報ACp)が受理される(ステップS156)。

【0129】そうすると、メモリカード110のコントローラ1420は、受理したライセンス(ライセンスID、コンテンツID、ライセンス鍵Kc1、アクセス制御情報ACm、および再生制御情報ACp)を、ライセンス領域1415Aに格納する(ステップS160)。そして、配信サーバ10において、課金処理が行なわれる。すなわち、配信制御部315は、課金情報を課金データベース302に記録する(ステップS162)。なお、この場合の試聴用ライセンスの配信に対する課金料金は、後述する本体用ライセンスの配信に対する課金料金よりも低い。そして、ライセンスの配信動作は終了する(ステップS164)。

【0130】暗号化コンテンツデータ{Dc}Kcについては、単なるダウンロード処理であるため詳細には説明しないが、試聴用ライセンスの配信動作が終了した後、携帯電話機100のコントローラ1109は、暗号化コンテンツデータの配信要求を配信サーバ10へ送信し、配信サーバ10は、暗号化コンテンツデータの配信要求を受信する。そして、配信サーバ10の配信制御部315は、情報データベース304より、暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infを取得して、これらのデータをバスBS1および通信装置350を介して出力する。

【0131】携帯電話機100は、{Dc}Kc//Dc-infを受信して、暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infを受理する。そうすると、コントローラ1106は、暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infをバスBS2およびメモリカードインタフェース1200を介してメモリカード110に入力する。メモリカード110のコントローラ1420は、受理した暗号化コンテンツ

10

20

30

40

50

データ {Dc} Kc および付加情報 Dc - inf をメモリ 1415 のデータ領域 1415B に記録する。なお、付加情報 Dc - inf には、暗号化コンテンツデータ {Dc} Kc のうち、どのブロックをどのライセンス鍵によって復号すべきかを示すライセンス鍵を変更するためのライセンスとブロックの対応情報とが含まれる。

【0132】このようにして、ライセンスの配信においては、携帯電話機 100 に装着されたメモリカード 110 が正規の認証データを保持する機器であること、同時に、クラス証明書 Cm3 とともに暗号化して送信できた公開暗号鍵 Kpm3 が有効であることを確認した上でコンテンツデータを配信することができ、不正なメモリカードへのコンテンツデータの配信を禁止することができる。

【0133】さらに、配信サーバおよびメモリカードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

【0134】なお、上記において、試験用ライセンスの配信に対して課金するとして説明したが（ステップ S162）、試験は、本体用ライセンスをダウンロードしてもらうことを目的としたサービスであり、より多くのユーザに聴いてもらう必要があるため、試験用ライセンスの配信に対しては課金をしないことも可能である。

【0135】〔試験〕次に、ステップ S20 における試験について詳細に説明する。試験用の再生においては、携帯電話機 100 のコントローラ 1109 は、メモリカード 110 から再生を行なう楽曲の付加データ Dc - inf を読出して、試験用ライセンスにて再生可能な試験用領域 {Dc1} Kc1 を構成するブロックを特定し、特定されたブロックのみにて構成される 1 つの新しい暗号化コンテンツデータを仮想的に生成し、この仮想的に生成された暗号化コンテンツデータを復号して再生する。図 3 の (a) を参照して、暗号化コンテンツデータ {Dc} Kc が暗号化コンテンツデータ 90 である場合には、試験領域 91 ({Dc1} Kc1) を構成するブロックを確認し、該当するブロックのみから構成されるデータ列を一つの楽曲として再生する。図 3 の (b) を参照して、暗号化コンテンツデータ {Dc} Kc が暗号化コンテンツデータ 93 である場合も同様に、試験領域 94 ({Dc1} Kc1) を一つの楽曲として再生する。

【0136】再生は、まず、メモリカード 110 に格納されている試験用ライセンスに含まれるライセンス鍵 Kc1 をコンテンツ再生回路 1550 内の 2 つの Kc 保持部 1514、1515 のいずれかに保持させる「再生許諾」と、「再生許諾」後に、Kc 保持部 1514、15

15 のいずれかに保持されているライセンス鍵 Kc1 をスイッチ 1518 にて選択して復号処理部 1519 に供給する。試験用に仮想的に構成された暗号化コンテンツデータは試験用領域 {Dc1} Kc1 と対応する。したがって、試験用に仮想的に構成された暗号化コンテンツデータを、暗号化コンテンツデータ {Dc1} Kc1 とも表すものとする。

【0137】そうすると、コントローラ 1109 はメモリカード 110 から暗号化コンテンツデータ {Dc1} Kc1 を構成するブロックを再生順序に従って読出して復号処理部 1519 に供給する。復号処理部 1519 は、入力された暗号化コンテンツデータを構成するブロックをライセンス鍵 Kc1 によって、それぞれ復号し、暗号化コンテンツデータ {Dc1} Kc1 を復号して得られるコンテンツデータを構成する平文化されたブロック（源データを構成するブロック）を抽出する。そして、復号処理部 1519 は、抽出したブロックを音楽再生部 1520 に出力する。音楽再生部 1520 は、復号処理部 1519 から供給されるブロックに含まれるデータに基づいて、音楽をデジタル再生し、AD変換器 1521 へ供給する。そうすると、AD変換器 1521 は、コンテンツデータをデジタル信号からアナログ信号に変換して端子 1522 へ出力する。そして、暗号化コンテンツデータ {Dc1} Kc1 を構成する全てのブロックが再生順に、メモリカード 110 から読出され、一連の処理が終了すると試験用の再生が終了する。ユーザは、端子 1522 に接続されたヘッドホン 130 等によってこの暗号化コンテンツデータ {Dc} Kc の試験領域 {Dc1} Kc1 を試験することができる。

【0138】このとき、再生の対象となる全てのブロックに対する一連の処理が終了すると試験用の再生が終了すると説明したが、繰り返し試験することを前提として、再生の対象となる全てのブロックの読出しが終了することも可能である。この場合、試験の終了は、ユーザが操作パネル 1111 を操作して、試験の終了をコントローラ 1109 に指示し、コントローラ 1109 が、指示に従って再生を終了するように構成する。

【0139】次に、試験用ライセンスに含まれるライセンス鍵 Kc1 をコンテンツ再生回路 1550 内の 2 つの Kc 保持部 1514、1515 のいずれかに保持させる「再生許諾」について説明する。図 12 は「再生許諾」の動作を説明するためのフローチャートである。「再生許諾」は試験用ライセンスのライセンス鍵 Kc1 を Kc 保持部 1514、1515 のいずれかに保持させるのみでなく、本体用ライセンスのライセンス鍵 Kc2 を Kc 保持部 1514、1515 のいずれかに保持させる処理でもあり、図 12 ではライセンス鍵は Kc i と表記されている。試験においてはライセンス鍵を区別する識別子

i が i = 1 と読替えて説明を行なう。また、ライセンス鍵 Kc 1 は Kc 保持部 1514 に保持されるものとして説明を行なう。

【0140】図 12 を参照して、試聴のための再生動作が開始されると、携帯電話機 100 のユーザから操作パネル 1111 を介して再生許諾リクエストが携帯電話機 100 にインプットされる (ステップ S200)。そうすると、コントローラ 1109 は、バス BS2 を介して認証データの出力要求をコンテンツ再生回路 1550 に行ない (ステップ S202)、コンテンツ再生回路 1550 は認証データの出力要求を受信する (ステップ S204)。そして、認証データ保持部 1500 は、認証データ {Kpp1//Cp1} KPa を出力し (ステップ S206)、コントローラ 1109 は、メモリカードインタフェース 1200 を介してメモリカード 110 へ認証データ {Kpp1//Cp1} KPa を入力する (ステップ S208)。

【0141】そうすると、メモリカード 110 は、認証データ {Kpp1//Cp1} KPa を受理し、復号処理部 1408 は、受理した認証データ {Kpp1//Cp1} KPa を、KPa 保持部 1414 に保持された公開認証鍵 KPa によって復号し (ステップ S210)、コントローラ 1420 は復号処理部 1408 における復号処理結果から、認証処理を行なう。すなわち、認証データ {Kpp1//Cp1} KPa が正規の認証データであるか否かを判断する認証処理を行なう (ステップ S212)。復号できなかった場合、ステップ S260 へ移行し、再生動作は終了する。認証データが復号できた場合、コントローラ 1420 は、セッションキー発生部 1418 を制御し、セッションキー発生部 1418 は、再生セッション用のセッションキー Ks2 を発生させる (ステップ S214)。そして、暗号処理部 1410 は、セッションキー発生部 1418 からのセッションキー Ks2 を、復号処理部 1408 で復号された公開暗号鍵 Kpp1 によって暗号化した {Ks2} Kp1 をバス BS4 へ出力する。そうすると、コントローラ 1420 は、インタフェース 1424 および端子 1426 を介してメモリカードインタフェース 1200 へ {Ks2} Kp1 を出力する (ステップ S216)。携帯電話機 100 のコントローラ 1109 は、メモリカードインタフェース 1200 を介して {Ks2} Kp1 を取得する。そして、コントローラ 1109 は、{Ks2} Kp1 をバス BS2 を介してコンテンツ再生回路 1550 の復号処理部 1504 へ与え (ステップ S218)、復号処理部 1504 は、Kp1 保持部 1502 から出力された、公開暗号鍵 Kpp1 と対になっている秘密復号鍵 Kp1 によって {Ks2} Kp1 を復号し、セッションキー Ks2 を暗号処理部 1506 へ出力する (ステップ S220)。そうすると、セッションキー発生部 1508 は、再生セッション用のセッションキー Ks3 を発生させ、

セッションキー Ks3 を暗号処理部 1506 へ出力する (ステップ S222)。暗号処理部 1506 は、セッションキー発生部 1508 からのセッションキー Ks3 を復号処理部 1504 からのセッションキー Ks2 によって暗号化して {Ks3} Ks2 を出力し (ステップ S224)、コントローラ 1109 は、バス BS2 およびメモリカードインタフェース 1200 を介して {Ks3} Ks2 をメモリカード 110 へ出力する (ステップ S226)。

【0142】そうすると、メモリカード 110 の復号処理部 1412 は、端子 1426、インタフェース 1424、およびバス BS4 を介して {Ks3} Ks2 を入力する。復号処理部 1412 は、セッションキー発生部 1418 によって発生されたセッションキー Ks2 によって {Ks3} Ks2 を復号して、再生端末 100 で発生されたセッションキー Ks3 を受理する (ステップ S228)。

【0143】携帯電話機 100 のコントローラ 1109 は、メモリカード 110 から事前に取得した再生リクエスト曲のライセンス管理ファイルからライセンスの格納されているエントリ番号を取得し (ステップ S230)、メモリカードインタフェース 1200 を介してメモリカード 110 へ取得したエントリ番号とライセンスの出力要求を出力する (ステップ S232)。

【0144】メモリカード 110 のコントローラ 1420 は、エントリ番号とライセンスの出力要求とを受理し、エントリ番号によって指定された領域に格納されたライセンスを取得する (ステップ S234)。

【0145】そして、コントローラ 1420 は、アクセス制限情報 ACm を確認する (ステップ S236)。

【0146】ステップ S236 においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報 ACm を確認することにより、具体的には、再生回数を確認することにより、既に再生不可の状態である場合には再生動作を終了し、アクセス制限情報の再生回数に制限がある場合にはアクセス制限情報 ACm の再生回数を変更した (ステップ S238) 後に次のステップ (ステップ S240) に進む。一方、アクセス制限情報 ACm の再生回数によって再生が制限されていない場合には、ステップ S238 はスキップされ、アクセス制限情報 ACm の再生回数は変更されることなく処理が次のステップ (ステップ S240) に進行される。

【0147】ステップ S236 において、当該再生動作において再生が可能であると判断された場合には、メモリ 1415 のライセンス領域 1415A に記録された再生リクエスト曲のライセンス鍵 Kc1 および再生制御情報 ACp がバス BS4 上へ出力される (ステップ S240)。

【0148】得られたライセンス鍵 Kc と再生制御情報 ACp は、切換スイッチ 1446 の接点 Pf を介して暗

号化処理部 1406 に送られる。暗号化処理部 1406 は、切換スイッチ 1442 の接点 Pb を介して復号処理部 1412 より受けたセッションキー Ks3 によって切換スイッチ 1446 を介して受けたライセンス鍵 Kc1 と再生制御情報 ACp とを暗号化し、{Kc1//ACp} Ks3 をバス BS4 に出力する (ステップ S240)。

【0149】バス BS4 に出力された暗号化データは、インタフェース 1424、端子 1426、およびメモリカードインタフェース 1200 を介して再生端末 102 に送出される。

【0150】携帯電話機 100 においては、メモリカードインタフェース 1200 を介してバス BS2 に伝達される暗号化データ {Kc//ACp} Ks3 を復号処理部 1510 によって復号処理を行ない、ライセンス鍵 Kc および再生制御情報 ACp を受理する (ステップ S242、S244)。復号処理部 1510 は、ライセンス鍵 Kc (この場合はライセンス鍵 Kc1) をスイッチ 1511 へ出力する。

【0151】また、復号処理部 1510 は、再生制御情報 ACp をバス BS2 に出力する。コントローラ 1109 は、バス BS2 を介して、再生制御情報 ACp を受理して再生の可否の確認を行なう (ステップ S246)。

【0152】ステップ S246 においては、再生制御情報 ACp によって再生不可と判断される場合には、端子 1512 にライセンス鍵 Kci を出力するようにスイッチ 1511 に指示し、Kc 保持部 1514 はライセンス鍵 Kci を保持する。

【0153】このようにして、Kc 保持部 1415 にライセンス鍵 Kc1 が保持され、「再生許諾」の処理が終了すると、暗号化コンテンツデータ {Dc1} Kc1 が再生可能となる。一方、ステップ S212、S236 および S246 によって分岐し、Kc 保持部 1415 にライセンス鍵 Kc1 が保持されないまま「再生許諾」が終了すると、暗号化コンテンツデータ {Dc1} Kc1 が再生できない。

【0154】したがって、たとえ暗号化コンテンツデータ {Dc} Kc の一部である試聴領域 {Dc1} Kc1 のみの再生であっても正規のライセンスを所持しないユーザが再生することはできない構成になっている。もちろん、暗号化コンテンツデータ {Dc} Kc を何らかの手段で取得し、その取得した暗号化コンテンツデータ {Dc} Kc をコピーしたものであってもよい。試聴用ライセンスを配信サーバ 10 から取得すれば暗号化コンテンツデータ {Dc} Kc を再生可能である。

【0155】また、試聴においては試聴用ライセンスしか保持しないため、ライセンス鍵 Kc2 にて復号するように暗号化された試聴領域外のブロック、すなわち、本体領域 {Dc2} Kc2 は本体用ライセンスを取得しない限り、再生することはできない。

【0156】[本体用ライセンスの配信] 次に、ステップ S30 における本体用ライセンスのダウンロードについて詳細に説明する。本体用ライセンスのダウンロードは、試聴用ライセンスのダウンロードにおける処理と同様に、図 10 および図 11 のフローチャートに従って処理される。この場合、ライセンス鍵 Kc2 を含むライセンスのダウンロードであることから、ライセンス購入条件 AC には本体用ライセンスの購入であることを示す情報が含まれている。また、フローチャートにおけるライセンス鍵を区別する識別子 i を i=2、すなわちライセンス鍵 Kci を Kc2 に読替えればよく、説明が重複するので説明を省略する。

【0157】ここでは、本体用ライセンスを取得した後も、暗号化コンテンツデータの再生にはライセンス鍵 Kc1 を含む試聴用ライセンスを用いて再生するように説明したが、試聴用ライセンスにはアクセス制御情報 ACm に含まれる再生回数制限を利用し、例えば、3 回程度の回数制限を加えた上で、無償で配信し、本体用ライセンスとして 2 つのライセンス、すなわち、ライセンス鍵 Kc1 を含むライセンスとライセンス鍵 Kc2 を含むライセンスを同時に配信を行っても同様なサービスを提供することができる。この場合、携帯電話機 100 は、図 9 のステップ S30 において 2 つのライセンスの配信を受ける。つまり、図 10 および図 11 に示すフローチャートを 2 回処理することで取得することができる。

【0158】[再生] ステップ S30 によって本体用ライセンスをダウンロードし、2 つのライセンスをメモリカード 110 に格納した後に、2 つのライセンス鍵 Kc1、Kc2 を用いて暗号化コンテンツデータ {Dc} Kc を再生する処理について説明する。ここでは、説明を簡単にするためにライセンス鍵 Kc1 は Kc 保持部 1514 に、ライセンス鍵 Kc2 はライセンス保持部 1515 に保持されるものとして説明するが、これに限定されるものではなく逆であってもよい。

【0159】図 3 を参照して、暗号化コンテンツデータ 90 を再生する場合について説明する。コントローラ 1109 は、暗号化コンテンツデータ 90 に対する付加情報 Dc-inf を参照して、暗号化コンテンツデータ 90 において試聴用領域 91 に属するブロックと本体用領域 92 に属するブロックを特定する。

【0160】次に、再生順序に従って最初のブロックを再生するために必要なライセンス鍵 Kc2 を Kc 保持部 1515 に保持するための「再生許諾」を図 12 のフローチャートに従って行なう。この場合、図 12 のフローチャートにおけるライセンス鍵を区別する識別子 i を i=2、すなわちライセンス鍵 Kci を Kc2 に読替えればよく、試聴再生における「再生許諾」と同様であるため説明を省略する。

【0161】続いて、スイッチ 1518 に対して端子 1517 を選択して、Kc 保持部 1515 に保持されてい

るライセンス鍵 Kc2 を出力するように指示し、暗号化コンテンツデータ 90 を構成するブロックを再生順に従ってメモリカード 110 から読出して復号処理部 1519 に供給する。さらに、コントローラ 1109 は、暗号化コンテンツデータ 90 を構成するブロックを、コンテンツデータの再生が連続して行なわれるように復号処理部 1519 に供給しつつ、その処理の空き時間を利用して、もう一つのライセンス鍵であるライセンス鍵 Kc1 を Kc 保持部 1514 に保持させる「再生許諾」を試聴用領域 91 に属するブロックの供給が開始される以前に行なう。ライセンス鍵 Kc1 に対する「再生許諾」は試聴における再生を行なう場合の「再生許諾」と同様であるので説明は省略する。

【0162】そうすると、コントローラ 1109 は、暗号化コンテンツデータ 90 を構成するブロックをメモリカード 110 から読み出して、再生順に供給し、試聴用領域 91 に達すると、スイッチ 1518 に対して端子 1516 を選択して Kc 保持部 1514 に保持されているライセンス鍵 Kc1 を復号処理部 1519 に出力するように指示し、引き続いて、暗号化コンテンツデータ 90 を構成するブロックを再生順に従ってメモリカード 110 から読出して復号処理部 1519 に供給する。

【0163】そして、再び、本体用領域 92 に達すると、再びスイッチ 1518 に対して端子 1517 を選択して Kc 保持部 1515 に保持されているライセンス鍵 Kc2 を復号処理部 1519 に出力するように指示し、引き続いて、暗号化コンテンツデータ 90 を構成するブロックを再生順に従ってメモリカード 110 から読出して復号処理部 1519 に供給する。すべてのブロックが供給されると、暗号化コンテンツデータ 90 の再生が終了する。

【0164】さらに、図 3 を参照して、暗号化コンテンツデータ 93 を再生する場合について説明する。暗号化コンテンツデータ 93 では、再生順に従うと、最初にライセンス鍵 Kc1 によって再生する試聴用領域 94 が存在する。従って、まず、ライセンス鍵 Kc1 を Kc 保持部 1514 に保持させる「再生許諾」を行なう。次いで、コントローラ 1109 は、暗号化コンテンツデータ 93 を構成するブロックをメモリカード 110 から読み出して、再生順に復号処理部 1519 に供給する。さらに、コントローラ 1109 は、暗号化コンテンツデータ 93 を構成するブロックを、コンテンツデータの再生が連続して行なわれるように復号処理部 1519 に供給しつつ、その処理の空き時間を利用して、もう一つのライセンス鍵であるライセンス鍵 Kc2 を Kc 保持部 1515 に保持させる「再生許諾」を本体用領域 95 に属するブロックの供給が開始される以前に行なう。

【0165】本体用領域 95 に達すると、スイッチ 1518 に対して、端子 1517 を選択して Kc 保持部 1514 に保持されているライセンス鍵 Kc2 を復号処理部

1519 に出力するように指示し、引き続いて、暗号化コンテンツデータ 93 を構成するブロックを再生順に従ってメモリカード 110 から読出して復号処理部 1519 に供給する。すべてのブロックが供給されると、暗号化コンテンツデータ 93 の再生が終了する。

【0166】図 1 に示すパーソナルコンピュータ 50 が配信サーバ 10 または CD-ROM 60 から暗号化音楽データ {Dc} Kc のみを取得して、カードライタ 80 を介してメモリカード 110 に格納することもできる。この場合、図 9 のステップ S10 における暗号化コンテンツデータのダウンロード処理が省略される。

【0167】また、図 1 に示すパーソナルコンピュータ 50 は、試聴用の暗号化音楽データ {Dc1} Kc1、本体用の暗号化音楽データ {Dc2} Kc2、およびライセンス鍵 Kc1 を含む試聴用ライセンスを配信サーバ 10 または CD-ROM 60 から取得して、カードライタ 80 を介してメモリカード 110 に格納することができる。この場合、図 9 のステップ S10 をパーソナルコンピュータ 50 が行ない、パーソナルコンピュータ 50 からカードライタ 80 を介したメモリカード 110 へのライセンスの格納は、図 10 および図 11 に示すフローチャートに従って行なわれる。この場合、パーソナルコンピュータ 50 は、図 10 および図 11 における配信サーバ 10 と携帯電話機 100 の機能を果たす。そして、携帯電話機 100 のユーザは、カードライタ 80 からメモリカード 110 を抜き、携帯電話機 100 に装着し、図 12 に示すフローチャートに従って暗号化音楽データ {Dc} Kc の試聴領域 {Dc1} Kc1 を試聴する。その後、暗号化音楽データ {Dc} Kc を聴きたいとき、携帯電話機 100 によって配信サーバ 10 から本体用の暗号化音楽データ {Dc2} Kc2 を復号するためのライセンス鍵 Kc2 を図 10 および図 11 に示すフローチャートに従ってダウンロードする。そして、携帯電話機 100 は、ユーザの再生要求に応じて、2 つのライセンス鍵 Kc1、Kc2 を用いて暗号化音楽データ {Dc} Kc の全てを再生する。また、説明を省略したが、配信サーバ 10 から試聴用ライセンスの取得、あるいは CD-ROM 60 への試聴用ライセンスの記録および試聴用ライセンスの読出しは暗号技術を用いて安全性が確保されているものとする。ただし、ここでは、その方法については限定しないものとする。さらに、本体用ライセンスをコンピュータ 50 にて配信サーバ 10 から受信してカードライタ 80 を介してメモリカード 110 に格納することも可能である。

【0168】このように、携帯電話機 100 は、各種の経路から暗号化音楽データ {Dc} Kc、およびライセンス鍵 Kc1、Kc2 をそれぞれ含む 2 つのライセンスを受信してメモリカード 110 に記録する。したがって、携帯電話機 100 のユーザが暗号化音楽データ {Dc} Kc の全てを再生できる状態でのダウンロードを希

望したとき、メモリカード 110 には、最終的に、暗号化音楽データ {Dc} Kc、およびライセンス鍵 Kc 1、Kc 2 をそれぞれ含む 2 つのライセンスが格納される。

【0169】上記においては、暗号化コンテンツデータが音楽データを暗号化した暗号化コンテンツデータである場合について説明したが、暗号化コンテンツデータが他の朗読データ、教材データ、およびビデオデータ等であっても上述した方法によって暗号化コンテンツデータのダウンロード、試聴、試写および再生を行なう。

【0170】本発明の実施の形態によれば、複数のブロックに分割された暗号化コンテンツデータと、複数のブロックに含まれる暗号化データを復号するための複数のライセンスとを配信するので、各ブロックを異なるライセンスによって復号および再生できる。その結果、配信されるライセンスに応じて課金料金を設定できる。

【0171】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【0172】

【発明の効果】本発明によれば、複数のブロックに分割された暗号化コンテンツデータと、複数のブロックに含まれる暗号化データを復号するための複数のライセンスとを配信するので、各ブロックを異なるライセンスによって復号および再生できる。

【図面の簡単な説明】

【図 1】 データ配信システムを概念的に説明する概略図である。

【図 2】 図 1 に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図 3】 暗号化コンテンツデータのフォーマットを示す図である。

【図 4】 暗号化コンテンツデータの生成方法を説明するための図である。

【図 5】 図 1 に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図 6】 図 1 に示すデータ配信システムにおける配信サーバの構成を示す概略ブロック図である。

【図 7】 図 1 に示すデータ配信システムにおける携帯電話機の構成を示す概略ブロック図である。

【図 8】 図 1 に示すデータ配信システムにおけるメモリカードの構成を示す概略ブロック図である。

【図 9】 図 1 に示すデータ配信システムにおける配信動作の全体構成を説明するためのフローチャートである。

【図 10】 図 9 に示すライセンスの配信動作をさらに詳細に説明するための第 1 のフローチャートである。

【図 11】 図 9 に示すライセンスの配信動作をさらに詳細に説明するための第 2 のフローチャートである。

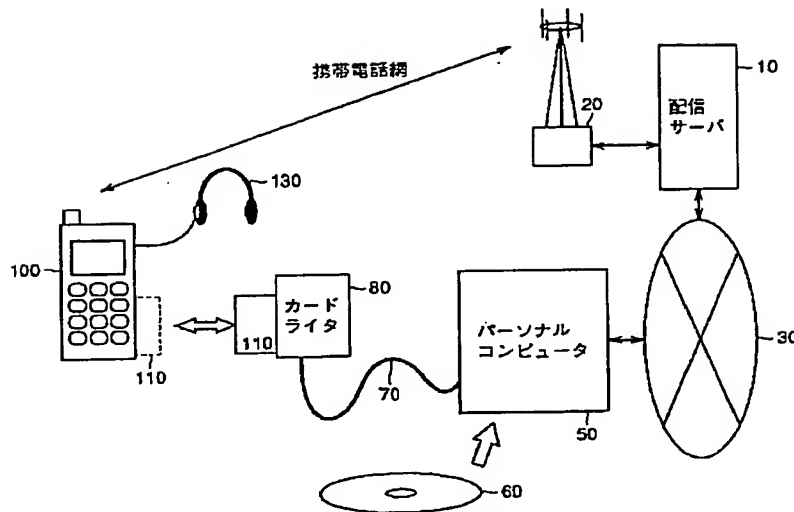
【図 12】 再生許諾動作におけるライセンス鍵の読出を詳細に説明するためのフローチャートである。

10 【図 13】 暗号化コンテンツデータの別のフォーマットを示す図である。

【符号の説明】

10 配信サーバ、20 配信キャリア、30 インターネット網、50 パーソナルコンピュータ、60 CD、70 USB ケーブル、84、90、93、96、97 暗号化コンテンツデータ、81 源データ、82 ブロックデータ、83、91、92、94、95、842、844、846 暗号化音楽データ 100 携帯電話機、110 メモリカード、130 ヘッドホン、302 課金データベース、304 情報データベース、307 メニューデータベース、308 配信記録データベース、310 データ処理部、312、320、1404、1408、1412、1422、1504、1510、1519 復号処理部、313 認証鍵保持部、315 配信制御部、316、1418、1508 セッションキー発生部、318、326、328、1406、1410、1417、1506 暗号処理部、350 通信装置、841、843、845、971、972 暗号化データ、961~967 領域、1109、1420 コントローラ、1426、1512、1513、1516、1517、1522 端子、1101 アンテナ、1102 送受信部、1103 マイク、1104 AD 変換器、1105 音声符号化部、1106 音楽再生部、1108 スピーカ、1110 表示パネル、1111 操作パネル、1200 メモリカードインタフェース、1400、1500 認証データ保持部、1402 Km c 保持部、1414 KPa 保持部、1415 メモリ、1415A ライセンス領域、1415B データ領域、1416 KPmc 保持部、1421 Km 保持部、1424 インタフェース、1442、1446 切換スイッチ、1502 Kp1 保持部、1520 音楽再生部、1107、1521 DA 変換器、1514、1515 Kc 保持部、1550 コンテンツ再生回路。

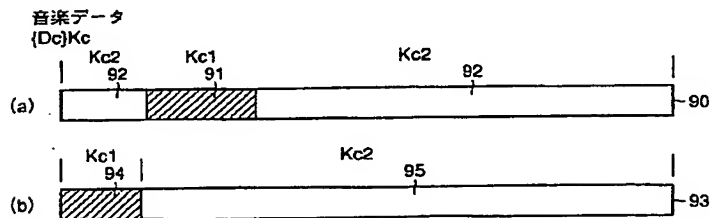
【図1】



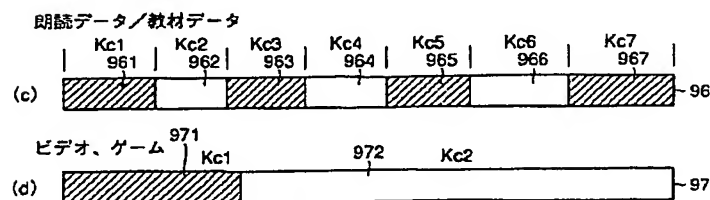
【図2】

記号	種類	属性	特性
Dc	コンテンツデータ	コンテンツ固有	例：音楽データ、朗読データ、教材データ、画像データ Kcにて復号可能な暗号化コンテンツデータ {Dc}Kcとして配信され、メモリカードに保持される
Dc-Inf	付加情報	コンテンツ固有	Dcに付随する平文データ。
Kc	ライセンス	コンテンツ固有	ライセンス 暗号化コンテンツデータを復号する復号鍵
ACm/ACp	ライセンス	ライセンス固有	制限情報 再生やライセンスの取り扱いに対する制限事項
ライセンスID	ライセンス	ライセンス固有	ライセンスを特定するための管理コード
コンテンツID	ライセンス	コンテンツ固有	コンテンツを特定するための管理コード
ライセンス	ライセンス	ライセンス固有	Kc+ACm+ACp+ライセンスID+コンテンツIDの総称

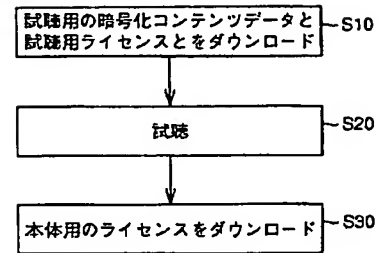
【図3】



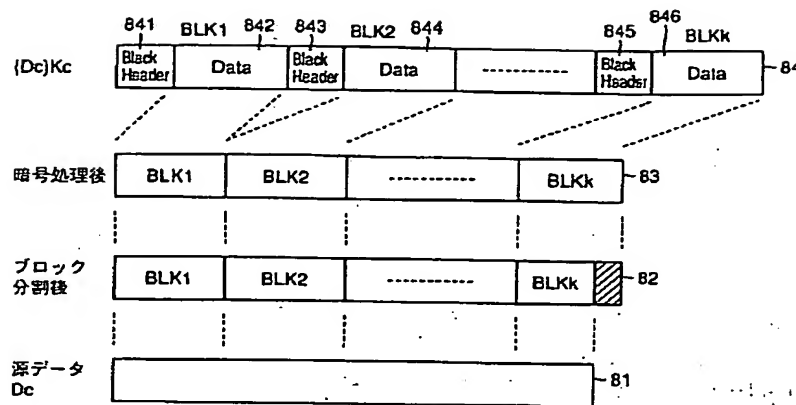
【図13】



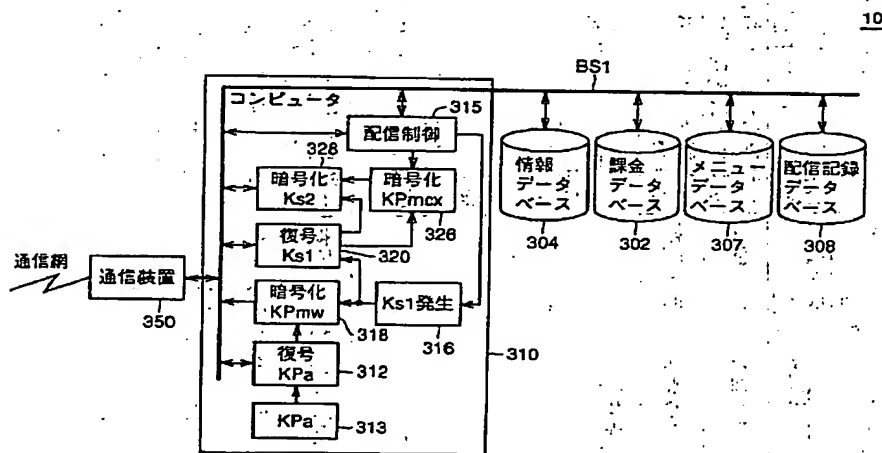
【図9】



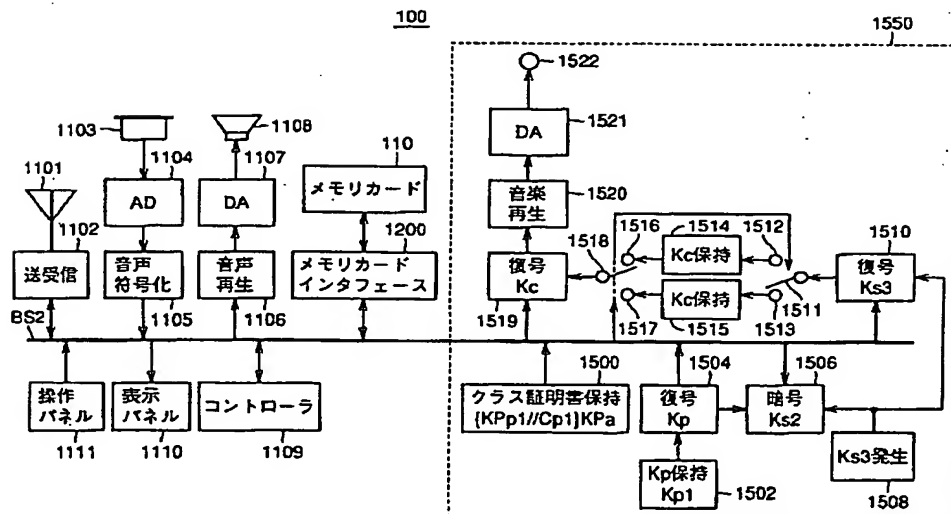
【図4】



【図6】



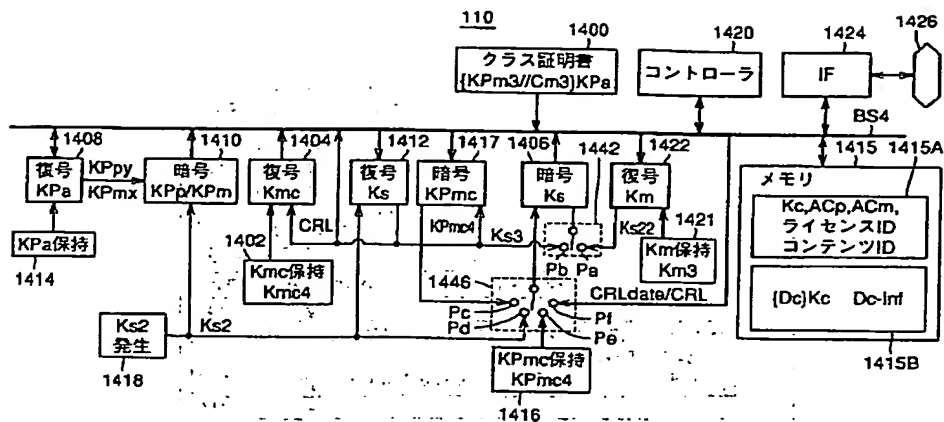
【図7】



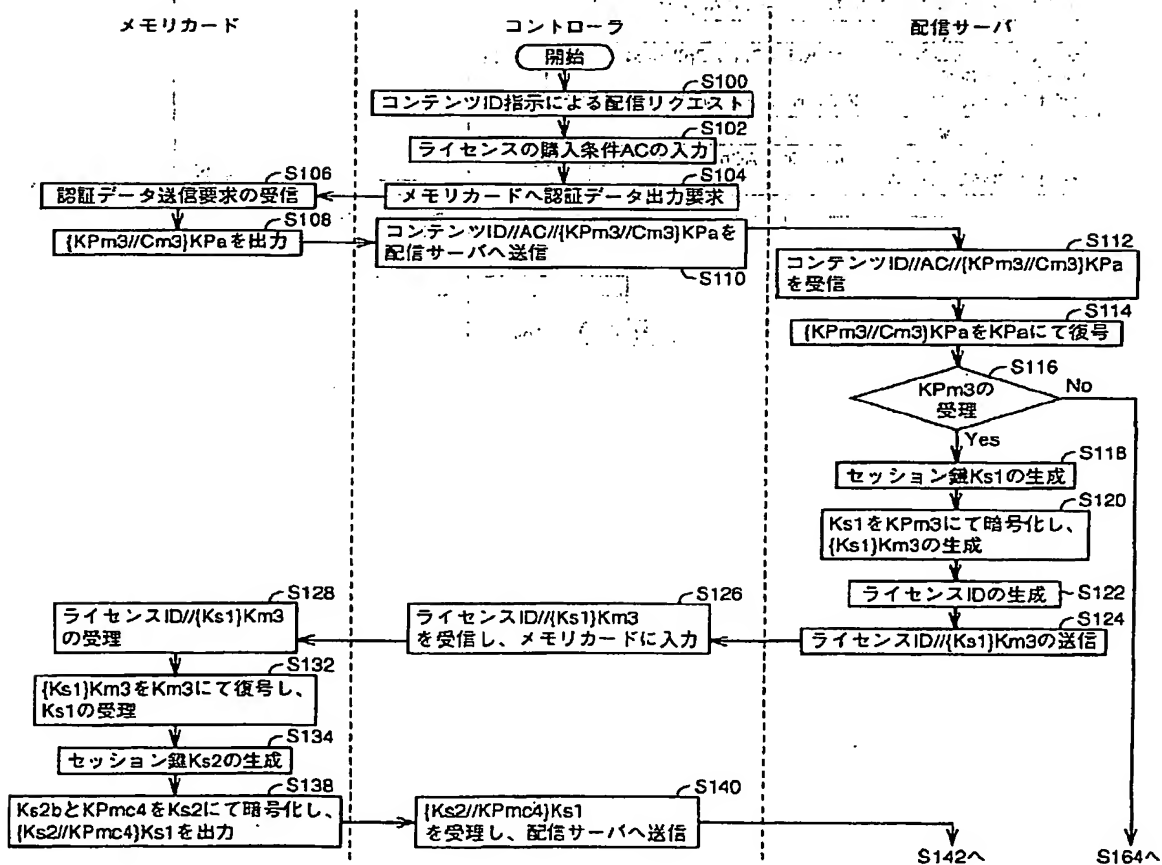
【図 5】

	記号	種類	属性	特性
配信サーバ	KPa	公開認証鍵	システム 共通	認証局にて認証データを復号する鍵
	Ks1	共通鍵	セッション 固有	メモリカードへのライセンシス配信ごとに発生
	KPa	公開認証鍵	システム 共通	認証局にて認証データを復号する鍵 配信サーバのKPaと同一
メモリカード	KPmw	公開暗号鍵	クラス固有	証明書Cmwとともに認証局にて暗号化された認証データとして保持 wはクラスを識別するための識別子
	Kmw	秘密復号鍵	クラス固有	公開暗号鍵KPmwにて暗号化されたデータを復号する非対称な 復号鍵
	KPmcx	公開暗号鍵	個別	メモリカードごとに異なる。 xはモジュールを識別するための識別子
	Kmcx	秘密復号鍵	個別	公開暗号鍵KPmcxにて暗号化されたデータを復号する非対称な 復号鍵
	Ks2	共通鍵	セッション 固有	配信サーバまたはコンテンツ再生回路間のライセンシスの授受ごとに 発生
	Cmw	証明書	クラス 証明書	メモリカードのクラス証明書。認証機能を有する。 {KPmw/Cmw}KPaの形式で出荷時に記録。 *メモリカードのクラスwごとに異なる。
	KPpy	公開暗号鍵	クラス固有	証明書Cmwとともに認証局にて暗号化された認証データとして保持 yはクラスを識別するための識別子
コンテンツ 再生回路	Kpy	秘密復号鍵	クラス固有	公開暗号鍵KPpyにて暗号化されたデータを復号する非対称な復号鍵
	Ks3	共通鍵	セッション 固有	メモリカード間の再生セッションごとに発生
	Cpy	証明書	クラス 証明書	コンテンツ再生デバイスのクラス証明書。認証機能を有する。 {KPpy/Cpy}KPaの形式で出荷時に記録。 *コンテンツ再生デバイスのクラスyごとに異なる。

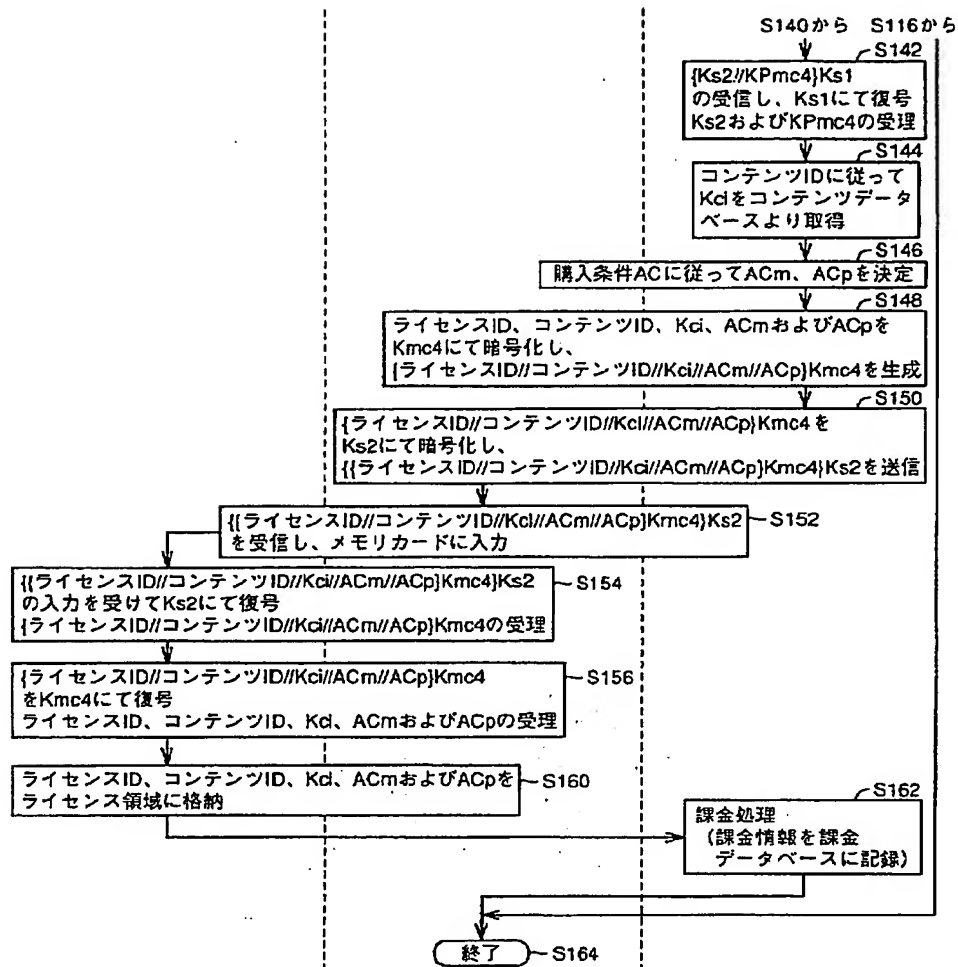
【圖 8】



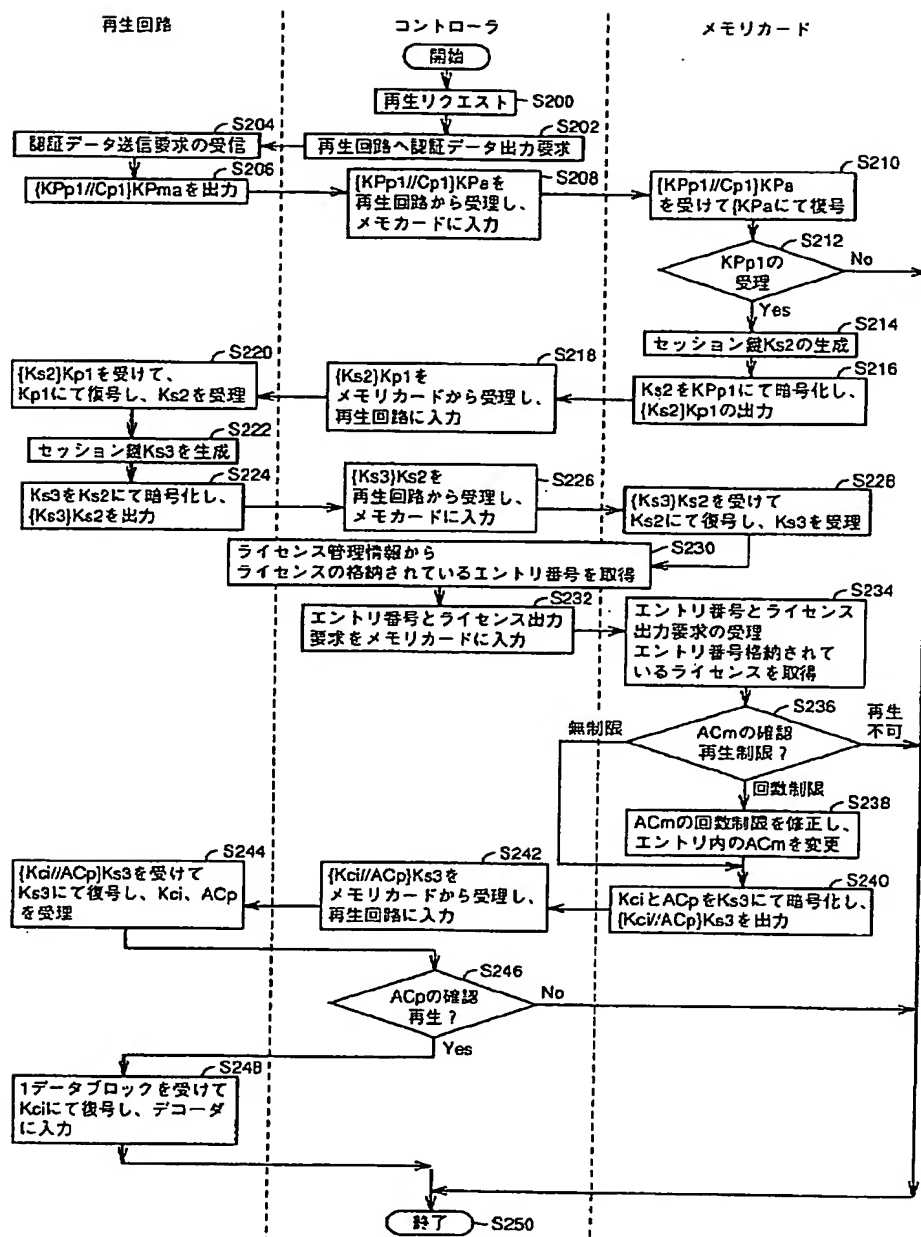
【図 1.0】



【図 11】



【図 12】



THIS PAGE BLANK (USPTO)